Securities (Signature Approver) Regulations, 5763-2003[1]

By virtue of our authority under section 44D(b) of the Securities Law, 5728-1968, in accordance with a proposal of the Authority, with the approval of the Scientific and Technological Research and Development Committee of the Knesset, we enact the following regulations:

Chapter 1: Interpretation

Definitions

1. In these regulations —

'Means of authenticating a signature', 'means of signature', 'electronic signature' and 'electronic certificate' — as defined in the Electronic Signature Law, 5761-2001 (hereafter — the Electronic Signature Law);

'Token' — a physical device that is connected to a port of the reporting computer, and which is used for the storage of a private key, a public key and an electronic certificate, which combined with a password known to the owner of the electronic certificate, allows authorized access to the reporting site of MAGNA;

'Reporting site' — the internet site of the Authority, to which the electronic reporting to the Authority is made [http://filing.magna.isa.gov.il];

'Distribution site' — the internet site of the Authority that is open for inspection by the public, where the reportings of the reporting bodies can be seen [www.magna.isa.gov.il];

'Reporting body' — a reporting corporation, a trustee of certificates of indebtedness within the meaning thereof in chapter 5A of the Law or an underwriter as defined in the Securities (Underwriting) Regulations, 5753-1993;

'Signature approver' — within the meaning thereof in section 44D(b) of the Law;

'MAGNA' (Electronic Fair Disclosure System)[2] — the Authority's

---

1 *Kovetz HaTakanot* (Collection of Regulations) 6231, 5763 (12 March 2003), p. 594.

computer system that is used for receiving and distributing the reportings of reporting bodies;

'Authorized electronic signatory' — within the meaning thereof in section 4D(b) of the Law;

'Technical document' — a document that includes technical requirements and work procedures for an approving body on MAGNA;

'Identifying number' — a code issued by the Authority, which is used for identification on MAGNA of a person whom the Authority approved to act as an authorized electronic signatory on behalf of a reporting body;

'Private key' — a means of signature with public key infrastructure (PKI) technology;

'Public key' — a means of authenticating a signature with PKI technology;

'Electronic Certificate Revocation List' — a file in accordance with standard ISO/IEC 594-8 as defined in the Electronic Signature Regulations, which contains a list of electronic certificates that were issued under these regulations and that were revoked before the date on which they expired, and also the date of the revocation and the reason for the revocation, if recorded (CRL — Certificate Revocation List);

'Directory Service' (DS) — a service for the identification, according to the standard, and the management of entities on a communications network, which is used by MAGNA;

'Registrar of Approving Bodies', 'register of approving bodies', 'database of valid electronic certificates' and 'database of revoked electronic certificates' — within the meaning thereof in the Electronic Signature Law;

'Reporting corporation' — including a corporation that files reports under Chapter 5C of the Law;

'The Electronic Signature Regulations' — the Electronic Signature (Secure Electronic Signature, Hardware and Software Systems and Scrutiny of Applications) Regulations, 5762-2001.

---

[2] MAGNA is an acronym of the Hebrew expression (מערכת גילוי נאות אלקטרונית) which means Electronic Fair Disclosure System.

Chapter 2: Approval to act as Signature Approver

Application to act as signature approver

2. (a) An approving body who wishes to act as a signature approver (hereafter — the applicant) shall submit an application in writing to the Authority at its office in Jerusalem; the application shall include all of the following:

(1) The name of the applicant, the name of the person designated to be the manager of the signature approver, the identity details of each of these and their addresses; if the applicant is a corporation, the application shall also include the documents according to which it was incorporated or according to which it operates, the details of the controlling owners of the corporation and the names of the members of the board of directors and the general manager, their identity details and their addresses;

(2) Details about the other occupations of the applicant.

(b) The following documents shall be attached to an application as stated in sub-regulation (a):

(1) Confirmation of the Registrar of Approving Bodies that the applicant is registered in the register of approving bodies under the Electronic Signature Law;

(2) A copy of the applicant's procedures document, as defined in the Electronic Signature Regulations, which has received the approval of the Registrar of Approving Bodies;

(3) Confirmation of the applicant that he has received from the Authority a copy of the technical document, that the requirements set out in the technical document are clear to him and that he has the skills and the means required to comply with these requirements;

(4) An undertaking in writing to deliver to the Authority six months' advance notice of an intention to cease acting as a signature approver.

Conditions for receiving approval to act as a signature approver

3. The Authority will approve a body to act as signature approver, if it complies with all of the following:

(1) It proves to the Authority's satisfaction that —

(a) It has the ability to act as a signature approver, and with regard to work with MAGNA, according to the technology, standards and procedures as the Authority shall direct from time to time in the technical document;

(b) It has the skills and the ability required in order to act in accordance with the provisions of chapter 3.

(2) It has deposited with the Authority a bank guarantee in the Authority's favour to guarantee compliance with its duties and undertakings under regulations 2(b)(4), 5(b), 10, 11 and 12(2); the guarantee shall be unconditional and irrevocable, not susceptible to being charged or attached, and its amount shall be, at all times, in accordance with the number of electronic certificates that the applicant has issued or intends to issue under these regulations, whichever is the greater, in accordance with the following amounts:

	In new sheqels
Up to 500 certificates	50,000
More then 500 but not more then 1,000 certificates	100,000
More than 1,000 certificates	150,000

(b) The Authority shall publish the fact that approval has been given to the signature approver and his details on the reporting site and the distribution site.

Identification of a signature approver on MAGNA

4. A signature approver, who has received the approval of the Authority under regulation 3, shall carry out, immediately after receipt thereof and also at any time upon the Authority's demand, the actions required in the DS, as the Authority shall direct in the technical document, so that MAGNA can identify the electronic certificates that he issues.

Reporting changes to the Authority

5. (a) An approving body must comply with all the conditions stated in regulation 3 as long as it acts as a signature approver.

(b) If a change occurs in one of the details that a signature approver submitted under regulation 2 or in its compliance with any of the conditions stated in regulation 3, it shall report this to the Authority within 24 hours of the time when it became aware for the first time of the change.

Cancellation of approval or temporary restriction of its validity

6. (a) If the Authority sees that a signature approver is not complying with any of the provisions of these regulations, it may, after giving the signature approver an opportunity to argue its case, revoke the approval that it gave to him; but the Authority may temporarily restrict, for a period that does not exceed 30 days, the validity of the approval instead of revoking it, if it sees that it is possible to amend what requires amendment in such a way that the signature approver can once again comply with the provisions of the regulations within the aforesaid time period.

(b) If the validity of the approval under sub-regulation (a) is restricted, and what requires amendment is not amended by the end of the period of the temporary restriction, the approval shall be revoked; however, if the Authority sees that the signature approver is taking reasonable steps in order to comply once more with the provisions of the regulations, it may extend the period of the temporary restriction for additional periods that do not cumulatively exceed thirty days, and to suspend until after these the revocation of the approval from coming into effect.

(c) Notwithstanding what is stated in sub-regulations (a) and (b), the Authority may revoke the validity of an approval that was given to a signature approver, even if he was temporarily restricted and the period of the temporary restriction has not yet ended.

(d) If the approval given to a signature approver is revoked or its validity is temporarily restricted, the Authority shall publish a notice of this on the reporting site and the distribution site.

Change of circumstances

7. (a) If the Authority sees that, because of a change of circumstances or a technological development that are not

within the control of the signature approver, he is no longer complying with the conditions stated in regulation 3(a), it may order him to act in order to comply with the conditions as stated within a period that it shall stipulate and in a manner that it shall stipulate.

(b) If a signature approver does not comply with the instructions of the Authority under sub-regulation (a), the Authority may temporarily restrict the validity of the approval or revoke it in accordance with regulation 6.

Chapter 3: Activity of Signature Approver

Issue of means of signature and electronic certificate

8. (a) A signature approver shall issue to an authorized electronic signatory of a reporting body, at its request, a private key and a electronic certificate for the purpose of electronic reporting to the Authority.

(b) A signature approver shall not issue a private key and an electronic certificate under sub-regulation (a) until he has identified the applicant and ascertained that he has a valid approval from the Authority for his registration on MAGNA, which includes an identifying number, and after he has received a notice by electronic mail from the Authority of the existence of such an identifying number; the signature approver shall receive and keep in his possession the said approval of the Authority with the other identification documents which he is obliged to keep in the manner and for the period determined for the identifying documents under the Electronic Signature Law.

(c) The private key and the electronic certificate that a signature approver issues as stated in sub-regulation (a) shall be stored on a password-protected token, which complies with the conditions as the Authority shall direct in the technical document; the procedure of creating the private key on the token shall be incapable of reconstruction, and shall ensure that the means of signature shall be under the exclusive control of the authorized electronic signatory from the moment it is created.

(d) An electronic certificate issued by a signature approver as stated in this regulation shall be in accordance with the provisions of the Electronic Signature Law and shall be made in the language, content, format and structure that the Authority directs in the technical document; the electronic certificate shall include, in addition to the details required under the Electronic Signature Law, also the identity details of the reporting body in whose name the authorized electronic signatory is entitled to report by means of that electronic certificate, and the electronic certificate shall state that the use thereof is designed only for the purpose of electronic reporting to the Authority in accordance with these regulations; no additional restriction shall be stipulated in the electronic certificate with regard to the use permitted of it with regard to electronic reporting to the Authority; the owner of the electronic certificate shall be the authorized electronic signatory.

(e) The validity of an electronic certificate issued under these regulations shall be for two years from its date of issue.

New issue of electronic certificate or renewed issue

9. (a) A new issue of an electronic certificate after its revocation or after the date of its expiry shall be done by a signature approver in accordance with the provisions of regulation 8.

(b) Renewed issue of an electronic certificate before the date of its expiry shall be done by a signature approver, based on an approval of the Authority that was given for the purpose of issuing the original electronic certificate, without any need to receive an additional approval from the Authority; the procedure of renewing the validity of an electronic certificate shall be identical to the procedure of issuing the original electronic certificate as stated in regulation 8, *mutatis mutandis*, and the renewed electronic certificate shall include all the elements that were included in the original electronic certificate, including the original public key.

(c) Renewal of the validity of an electronic certificate as stated in sub-regulation (b) shall be done in the period of thirty days before the date of its expiry; the signature approver shall send a warning to the owner of the electronic certificate, no later than forty-five days before the date of its expiry, and shall invite him to renew the validity of the certificate in the period

of the thirty days before the date of its expiry.

(d) The validity of an electronic certificate that was issued under these regulations shall not be renewed more than the number of times that the Authority shall stipulate in the technical document.

Transferring data to MAGNA about the issue or renewed issue of an electronic certificate

10. Without derogating from the provisions of any law concerning the management of a database of valid electronic certificates and a database of revoked electronic certificates, the signature approver shall transfer to the Authority, immediately after issuing any new electronic certificate under these regulations or after renewing the validity of an existing electronic certificate, the details of the electronic certificate that he issued or renewed, including the public key of the authorized electronic signatory to whom the electronic certificate was issued; transfer of the said data to the Authority shall be carried out directly to the DS via the Internet, by means of a designated point-to-point line or in another way, all of which as the Authority shall direct in the technical document, and shall end after receipt of the data by the DS.

List of revoked electronic certificates

11. (a) Without derogating from the provisions of any law concerning the management of a database of valid electronic certificates and a database of revoked electronic certificates, a signature approver shall transfer to the Authority the list of revoked electronic certificates, immediately after revocation of any electronic certificate that he issued under these regulations, and also with a frequency of at least once every two hours; the validity of the list of revoked electronic certificates transferred to the Authority shall be for 12 hours from the time of issue; the transfer of the list of revoked electronic certificates to the Authority shall be made directly to the DS via the Internet, by means of a designated point-to-point line or in another way, all of which as the Authority shall direct in the technical document, and shall end after receipt of the data by the DS; a temporary or permanent fault on the computers of the signature approver or on the communications lines shall not constitute a justification for a delay or postponement in transferring the list of revoked electronic certificates to the Authority.

(b) The access to the database of valid electronic certificates issued under these regulations, which is managed by a signature approver, shall not be open to public inspection.

Duties of signature approver

12. Without derogating from the provisions of any law concerning the activity of an approving body, the approving body shall comply, throughout the whole period of his activity as a signature approver, to the satisfaction of the Authority, with the following conditions:

(1) He shall act in accordance with the instructions of the Authority, which shall be given from time to time, and shall be set out in the technical document which shall be delivered to him, including with regard to the following subjects:

(a) The manner of setting up and maintaining the communications to the MAGNA site;

(b) The main actions required on the DS so that MAGNA shall be able to identify the electronic certificates issued by a signature approver, a stated in regulation 4;

(c) The conditions for the token, as stated in regulation 8(c);

(d) The language, content, format and structure of an electronic certificate issued under these regulations, as stated in regulation 8(d);

(e) The maximum number of times for renewing the validity of an electronic certificate issued under these regulations, as stated in regulation 9(d);

(f) The manner of transferring the data of the electronic certificate to MAGNA, as stated in regulation 10;

(g) The manner of transferring the list of revoked electronic certificates to MAGNA, as stated in regulation 11;

(h) The manner and conditions for converting an interface that operates with the main site of MAGNA to operate with the secondary site of MAGNA, and conditions for converting the interface back to operate with the main site of MAGNA;

(i) The level of service in the system of receiving telephone applications in so far as this concerns the installation and use of means of signature and the electronic certificate that were issued under these regulations, as stated in

paragraph (4) below;

(j) Dealing with exceptional situations that may occur at the stage of registering an authorized electronic signatory with a signature approver, at the stage of transferring data from a signature approver to MAGNA and at the stage of receiving and synchronizing the date on MAGNA;

(k) Additional instructions for an interface with MAGNA;

(2) He shall keep non-public information that comes into his knowledge as a result of his activity as a signature approver confidential, and he shall make no use of it except for the purpose of his activity as a signature approver, and he shall determine internal work procedures and adopt all the reasonable means for maintaining confidentiality by him, by his employees and by everyone who acts on his behalf with regard to the aforesaid information;

(3) He shall ensure the existence of a working computer communications line, by means of which he can establish and maintain a connection with the Authority;

(4) He shall ensure the existence of a help team and telephone service system for the benefit of reporting bodies, in so far as the installation and use of the means of signature and electronic certificate issued under these regulations are concerned, which shall be available 24 hours a day, except on Saturdays and Jewish festivals; the level of service in the telephone service system shall be according to the definitions that the Authority shall stipulate in the technical document;

(5) He shall provide a warranty for the means of signature, the electronic certificate and the tokens that he issues under these regulations, for a period of at least twelve months from their date of issue.

(6) He shall include on his internet site information about the location of his offices and the hours when they are open, and also a list of frequently asked questions (FAQ) and answers with explanations about his activity, including with regard to the procedures for issuing an electronic certificate for the purpose of electronic reporting to MAGNA, renewing its validity and revoking it; he shall also include on the site information about the extent of the warranty for the products

and services that he provides under these regulations, and installation instructions for the means of signature, the electronic certificate and the token in Hebrew and English, which include detailed explanations of the various work environments and work platforms;

(7) He shall ensure the possibility of immediately receiving by telephone notices about revocation of electronic certificates issued under these regulations 24 hours a day, every day of the year;

(8) He shall ensure the proper and full operation, during at least 99.95% of the hours of the day on an annual calculation, of the services required of him for the purpose of working with MAGNA, and also of the systems —

(a) Required for examining and updating the database of valid electronic certificates and the database of revoked electronic certificates that were issued for the purpose of electronic reporting to the Authority under these regulations;

(b) Used for the purpose of updating the Authority of the issue of a new electronic certificate or revocation of an existing electronic certificate.

Realization of guarantee

13. If a signature approver breaches one of his undertakings or does not comply with one of its duties under regulations 2(b)(4), 5(b), 10, 11 and 12(2), the Authority may, after giving the signature approver an opportunity to state his case, realize the bank guarantee that was deposited in its favour under regulation 3(a)(2).

Activity of a signature approver during a temporary restriction period or revocation of validity of the approval

14. (a) If the approval given to a signature approver is temporarily restricted as stated in regulation 6, the signature approver shall not issued a means of signature nor shall he renew the validity of existing electronic certificates for the purpose of electronic reporting to the Authority in accordance with the provisions of these regulations, as long as the validity of the approval given to him is temporarily restricted.

(b) If the validity of the approval given to an approving body to act as a signature approver is revoked, the approving body shall take the following steps:

(1) He shall refrain from issuing a means of signature nor shall he renew the validity of existing electronic certificates for the purpose of electronic reporting to the Authority in accordance with the provisions of these regulations;

(2) He shall notify, without delay, the owners of the existing electronic certificates that he issued under these regulations, of the revocation of the approval that the Authority gave to him, and he shall notify them that their electronic certificates will be revoked at the end of seven days from the date of the revocation of the approval, and that they must take steps to obtain a new electronic certificate from another signature approver;

(3) He shall revoke, at the end of seven days from the date of the revocation of the approval, all the electronic certificates that he issued under these regulations, and he shall enter them into the database of revoked certificates.

Chapter 4: Miscellaneous

Technical document

15. The Authority may, after consultation with the Registrar of Approving Bodies and after giving every signature approver an opportunity to state its case, change from time to time the technical document; a decision as to such a change shall be made, *inter alia*, after taking into account the cost involved in the change to a signature approver.

24 Adar I 5763 (26 February 2003)

Meir Sheetrit	Silvan Shalom
Minister of Justice	Minister of Finance