イスラエルにおける暗号関連動向調査 報告書
Contents

Question 1........................................................................................................................................5

To survey if there are any guidelines, etc. being prepared for the measures to be taken in case specific Cryptographic Algorithm is being compromised. When prepared, Surveryor to provide the concrete contents..................................................5

Question 2........................................................................................................................................9

To survey if there is any legal framework which will provide a certain legal effect onto Electronic signatures or time stamps using cryptographic technology. When those framework s exist, Surveyor to report the information concerning its contents and its review plan. When those framework does not exist, Surveyor to report a further plan to create legal framework. ........9

Question 3.......................................................................................................................................31

For the framework described above, to survey how the legal effect would be affected in case that the Algorithm is being compromised which is already used in electronic signatures or time stamps. Or Surveyor to report the schedule to which examination of a legal effect will be performed from now on. ......................................................................................31

Liabilities........................................................................................................................................33

Question 4.......................................................................................................................................36

To survey if Israel government investigate any technical countermeasures and legal countermeasures for breaking any cryptographic system, and with what member it is investigated. ..............................................................................................................36

Question 5.......................................................................................................................................44

Question 6.......................................................................................................................................46

To survey if Israel government validate the cryptographic product used in government organizations excepting the Department of Defense and the Ministry of Foreign Affairs. When the cryptographic product is validated, Surveyor to report if there are a requirement and evaluation Criteria, if it is opened to the venders. If opened to the public, Surveyor to report the contents.......................................................................................................................................46
Introduction

Not too long ago cryptography interested only mathematicians, and the military. Nowadays it seems to be of interest to many sectors. Every day we rely more and more on public networks to conduct both our personal lives and our business. Much of what we do is confidential, yet the networks we use promise no privacy whatsoever. Not only is it impossible to trust the network we use but it is becoming more and more difficult to be sure that our systems are not under attack or even compromised. At the same time, remote unauthorized access to computers is more and more common.

One of the most threatening and bothersome problems of the 2000's is the compromise of major cryptographic systems. This subject concerns both the leading companies and Israeli industry as a whole. It is understood that individual hackers and companies are trying to break into major systems, including the RSA and similar systems, everyday. In the light of this, we answered your questions in the hope that it would give you an understanding of the way the Israeli law system and government ministries are handling this issue.

In order to prepare this paper we used many resources:

We were in contact with the following institutes and people:

1. Ministry of Justice
2. The Ministry of Police – The Department for Computer Security
3. Ministry of Defense – Cryptology Department
4. Ministry of Treasury
5. Ministry of Commerce and Industry
6. ANC Company
7. A Certification Authority
8. Professor Adi Shamir,
9. Professor Michael Birenhak, Haifa University
10. Haim Revai, Advocate
11. Jonathan Agmon, Advocate
12. Adi Nordman, Advocate

Sources used for the completion of the paper:

2. The amendments for the Electronic Signature Law
3. Law of Computers
4. Cryptology Order
6. Court Rulings
7. Articles (were written in Hebrew and therefore not indicated).
Question 1

To survey if there are any guidelines, etc. being prepared for the measures to be taken in case specific Cryptographic Algorithm is being compromised. When prepared, Surveyor to provide the concrete contents.

Different interests motivate different entities to compromise specific cryptographic algorithms. The classic motivations are competition, R&D, crime, fraud or espionage. Some want fame, revenge or simply see a challenge in cracking ones system.

Thousands of penetration trials into civil cryptographic systems are reported in the Israeli computer crime security survey per week. Most of these trials happen after political events.

We checked among government authorities and other institutes and found that there are no specific guidelines for the measures to be taken in the event specific cryptographic algorithms are being compromised, with the exception of cases that refer to the general law, such as contract law (assuming that both sides signed the contract), commercial privacy law (on the condition that the material was kept secret), protection of privacy, and perhaps also tort law.

Yet, there are serious discussions among government and other authorities on how to act and which measures to take in case of a break-in to cryptographic systems. Owing to the lack of specific guidelines and because of the importance of the subject, different
institutes in Israel work towards preparing such guidelines.

The Israeli State comptroller warned in his annual report of 2002 that such guidelines are necessary. He pointed out the need for an authority that will coordinate the subject of data security in the different governmental computer services on a systematic basis. The comptroller stressed the complexity of the data security warfare.

In light of the State comptroller’s comments on the need for guidelines and the need for an authority to deal with data security, the government decided in September 2003 to establish a national committee to advance research in technologies for protecting civil infrastructure. This committee will submit its conclusions and suggestions to the Government in 2005.

At the end of 2002, a committee composed of lawyers, professors from the leading universities of law and computers, and law students was gathered in order to discuss attacks of terror in data information in the warfare arena.

The committee arrived at the following conclusions:

1. The committee rejects the existing approach in the cryptography guidelines which presents general bans, with specific exceptions that allow certain activities.

2. To overcome these approaches it is necessary to legislate a special cryptography law in Israel.

3. The purpose of such legislation is to have regulations on this subject and to keep an appropriate climate that suits the values of the State of Israel.
4. If the bill will be accepted it must bring into consideration the law of freedom of occupancy and so on.

In addition, the Israeli parliament established a committee to deal with the same subject with the title of “Homeland Security” concerning the government’s preparation in protecting the national infrastructure against terror attacks through the Internet. This committee raised problems concerning the lack of instructions in the event cryptographic systems are compromised and the existing national infrastructure exposed.

Different ideas were presented in the initial discussions of the committee such as the establishment of a framework for the absorption of information about attempts to break into cryptographic systems, and decisions on the preferable order of which cryptographic systems are worth protecting. This information will arrive from all governmental bodies who will report on the trials for penetration threats to which they are exposed. The report will include: the type of trails of penetration, its characteristics, its trends, the number of attempts to compromise the system and the level of sophistication of the trial for penetrations. The second stage will be an overall protection of databases. The Israeli government enables varied on-line services in their offices and the security of these sites is one of the most urgent issues.

In the last decade, private, public and government companies invested many resources in the subject of security policies. Over the years major companies use secured cryptographic systems, but it is clear in light of the relatively large number of
penetrations and break-in efforts into civil systems that guidelines need to be established for taking steps in the event that systems are compromised.

In spite of all these efforts, there are still no clear guidelines for a response in case major cryptographic systems are broken into. In some institutes it is thought that it is impossible to break into major cryptographic systems that exist in the market today. They cite as an example the continued attempts and competition to break into the RSA system, which no one has succeed in doing up until now. The different authorities take into consideration that even if someone compromises that system or others similar to it, it will be easy to quickly regain control and correct the cryptographic algorithms by lengthening the keys and adding measures to cancel this ability to penetrate before causing damage. In case of penetration the break-in will be published to the public, which will leave enough time to make the necessary changes and to protect the public.

Professor Adi Shamir, who was one of the developers of the RSA software and continually follows the subject agrees with this opinion.
Question 2

To survey if there is any legal framework which will provide a certain legal effect onto Electronic signatures or time stamps using cryptographic technology. When those framework s exist, Surveyor to report the information concerning its contents and its review plan. When those framework does not exist, Surveyor to report a further plan to create legal framework.

The law of electronic signature was legislated in Israel during 2001. The law, which was prepared by the Israeli Ministry of Justice years before, achieved legal authorization within the Israeli parliament after having been reviewed by different established committees, government offices, the Bar Association and other institutes which designed it to suit legal, commercial and technological needs.

Before getting into analysis of the law and its different paragraphs, we will detail:

1. The purposes of the law
2. What it intends to secure
3. The advantages
4. The disadvantages
5. The legal characteristics of the electronic signature

1. The purposes of the law

A. To make possible business transactions through electronic media, even when the parties are not acquainted with each other.
B. To ensure that formal demands of the law on electronic documents will be similar to those on written documents and written signatures.

C. To determine the liability for a document signed electronically and the liability between the parties of the electronically-signed document.

D. To ensure data integrity, its authenticity, and non-repudiation of the electronic document, as well as its purpose and the identity of its sender.

E. To preclude the need for a physical meeting between the parties.

F. To develop international electronic commerce and determine the rules and recognition of foreign electronic signatures. The use of signatures through foreign companies and electronic certificates, which are issued by a foreign Certification Authority, is quite common. In order to enable regular commerce within international business, the political, and legal systems need to issue, under certain conditions, validity for signatures or certificates issued by foreign authorities.

2. **What it intends to secure**

The law intends to secure transactions through the internet between people who had no former acquaintance or mutual cryptographic key, and to determine the possibility of fraud.

The law also determines the liability for a document signed electronically, or the liability between the parties of the electronically signed document. Parties of electronic commerce rely on electronic certificates, which are issued by different certification authorities. The legal system desires to supervise the certification
authorities in order to verify that the role will not be compromised and to ensure that the activities of the certification authority will be done in a way that preserves the integrity and authenticity of its products. This is how the process of recording the certification authorities and supervising their activities is processed.

It verifies the time of the certificate's dispatch and ensures that no changes were performed within it after it was dispatched. The electronic signature enables the existence of commercial relations within open computer nets, such as the Internet. In such transactions, often the parties don't know one other, and want to verify the identity of the other side. Barring a meeting with the other parties, there aren't any other external expressions for their agreement to accept the electronic message. The electronic signature can rectify this and other similar problems.

The Israeli law casts the responsibility on all parties (the signer, the Certification Authority and the receiver of the signature) who are involved in the electronic signature, depending on the performance. The signer, in particular, has an obligation to take reasonable means to secure the signature device, and to prevent unauthorized use if its signature's integrity becomes invalid. In that situation, he must notify all parties who rely on the signature including the Certification Authority. The signer will not be liable if he fulfilled these demands. The Certification Authority has to confirm and verify the identity of
the signer and the concerning details before issuing the certificate, as well as to conduct a reliable system for managing the database. In addition, the Certification Authority must revoke a certificate immediately when presented with a legal reason to do so. If the Certification Authority completes these obligations, it will not be liable for the damage of the reliability. In addition, the Certification Authority can explicitly limit the sum that can be transferred through the electronic certificate and may restrict the uses of the certificate to specific purposes only. If these conditions to obligate the signer or the Certification Authority are not met, the liability will fall on the party that depends on the signature.

3. **The advantages of the law**

The main advantage of the law is its flexibility. It leaves the regulations room to add and to change according to the futures needs. For example, the law does not determine an obligating strength of cryptographic keys for secured electronic signatures, but rather leaves it to the regulator.

Also the law isn’t set to the measures of any particular technology. Any technology that will meet the demands of integrity is acceptable. This enables to be neutral towards any type of technology, and allows the development of new technologies to be used as well.

4. **The disadvantages of law**
A. The possibility of losing control by breaking into the system where the signature is stored, or the theft or loss of an item connected to the signature such as a smart card is one disadvantage.
The solution for that is the use of a biometric identity marker or password in addition to the electronic signature.

B. Some scholars criticize methods of legislation that don't take into account the technology at the basis of the electronic signature, and thereby enabling the use of unreliable cryptographic means that can be easily decrypted. Thus, it was observed, it is possible to use a minimal standard of cryptography.

C. According to the law, only cryptographically secured signatures can be accepted by the official authorities, which means other electronic signatures have an inferior position. Yet accepting a cryptographically secured signature requires going through the bureaucratic process by giving all the personal details to the Certification Authority, which then goes through another bureaucratic process to supply two cryptographic keys. Some scholars criticize this process.

5. **The legal characteristics of electronic signature**
The model of electronic signature law in Israel defines three types of signatures, and recognizes the use of all electronic signatures as valid signatures. We define them as follows:

A. The simple electronic signature
B. The symmetric private secured electronic signature
C. The cryptographically secured and certified signature.

We will define each one as per the law:

A. The simple electronic signature is not cryptographic and could be an inserted symbol or scanned signature. This type of electronic signature can not be considered secure enough as it can not be ensured that the document hadn’t gone through any change and that the signature is really authentic. It is very easy to copy signatures and add them to a document, impersonating the owner of the signature.

B. The symmetric private secured electronic signature.

Traditional cryptography has usually involved two parties who create and share a secret key for the encryption and decryption of messages. This secret or private key system has a significant flaw. Sometimes the parties adopt a weak cryptographic key. If the key is discovered or intercepted by someone else, messages can easily be decrypted by other people who aren’t part of the deal. Therefore, even
though the law allows the usage of this type of electronic signature in the case of dispute, the general law will be implemented.

C. The cryptographically secured and certified signature. The asymmetric cryptography has a pair of mathematically related cryptographic keys. In this technology, each signer has a pair of mathematically related cryptographic keys. If one key is used to encrypt information, then only the related key can decrypt that information. One key is a unique private key under the sole control of the signer, and the other key is a unique public key that is freely distributed and can be seen by all users who receive the message. Before starting to use this kind of electronic signature, users must first receive a pair of cryptographic keys, a private and a public key, from an endorsing authority.

Cryptography is based on an irreversible mathematic algorithm connection between the keys, in order that it will be possible to reconstruct one key with the other key. The distribution of the public and private keys is done by different organizations that specialize in the subject and have the endorsement of the legal authorities, which is entitled a Certification Authority. The Certification Authority issues a
digitally-signed electronic certificate, which confirms the identity of the signer and refers him to the public key. Through this electronic certificate the recipient can be certain who communicated with him. It is also possible to enquire with the Certification Authority if the electronic certificate is valid. This type of signature is accepted by the law and recognized as the only signature that will be accepted.

The legislator issues a favored status to this signature which completes a certain set of essential demands that issue integrity guarantees. The uniqueness of the signatures identifying the key enables the existence of sole control of the signer on the means of signature and the ability to identify changes that were made in the document from the moment of its composition.

Therefore this model gains the status of a preferred electronic signature (“secured electronic signature”) even though it isn’t mentioned by name and the law doesn’t refer to it particularly.

The Law by Paragraphs

Paragraph 1 This paragraph gives definitions of the terms in the law, and defines the device that produces the secure electronic signature which is under the sole control of the signer. The law defines ‘the device’ as a unique software, object or information required for creating a secure electronic signature. The legislator made four rules for electronic signatures which are secured and certified:
1) It is unique to the owner of the Signing Device
2) It enables apparent identification of the owner of the Signing Device.
3) It is created using a Signing Device that can be maintained under the sole control of the owner of the Signing Device.
4) It enables identification of any change to the electronic message subject to signing.

**Paragraph 2** This paragraph makes the distinction between a signature that is demanded by law and a signature that isn't demanded by law. The law accepts the certified electronic signature as a valid legal signature when there is a legal demand for a signature.

**Paragraph 2(a)** The Israeli law determines that in addition to the electronic signature, it is necessary to verify the signature by a Certification Authority. The law sets a special status to a secured and verified electronic signature. Thus when the law demands a signature, it is possible to fulfill this demand only through a **secured and verified electronic signature**. A government office must register the Certification Authority provider. Only a certificate which is issued by an accredited Certification Authority can fulfill the conditions of the secure and verified electronic signature. Thus, where the law
demands a signature, it necessarily means that it also demands an electronic certificate, which is issued by the accredited Certification Authority.

**Paragraph 2(b)** This paragraph states that in some cases even a secured and verified electronic signature will not be accepted (an example is the inheritance laws, where it is written that the testament must be in writing, in the legislator’s handwriting and signed by him.

**Paragraph 3** This paragraph gives a special legal status to an electronic message signed by a secured electronic signature, that will be admissible in any legal process as alleged evidence that the signature is actually the signature of the signee and that the contents of the electronic commercial act were endorsed by the signee. Paragraph 3 sets the evidential status of an electronic message signed by a secure electronic signature and verifies it, ensuring that it is a message to a certain person and ensuring the contents of the message. This electronic message testifies better than any other witness on the contents of a written document and thus it is admissible in any legal process.

It must be noted that paragraph 3 of the law relates to the subject of legal admission of a similar status to both a secure electronic signature and a secure verified electronic signature. There were two explanations that were attached to the law. First, it is possible to issue and secure electronic signatures through technologies that will not necessitate electronic certificates; and second, the law doesn’t necessitate the registration of the Certification Authority.
The electronic message that is signed with a secured electronic signature is admissible. Theoretically two evidences are needed: one that the signature belongs to signer and two that the contents of the signed electronic message was accredited by the signer. In the secured electronic signature they are not need. These proofs will stand after the depending party will prove that the message was signed by a secured electronic signature, as defined by the law, and that the party to which the signature is attributed is in fact the signer. Because a secured electronic signature creates a clear affinity between the signer and the signature devices, and assures that no change was made in the signed message, it is possible to connect the signer to the message, which he signed. It is not a complete proof, but it shows a heavy burden on the signer to prove that the electronic message, which he signed, was not, in fact, signed by him, and a heavier burden on the signer who claims that he didn’t credit the contents of a document signed by him. A denial of an electronic message is much more difficult than a denial of a message which was signed regularly, on paper. It should also be noted that even if the signer is able to prove this, then if he didn’t, as the signer, use all the possible means for guarding the signature device and preventing unauthorized use, or if he didn’t deliver the message to someone he knows that relies upon his signature, immediately when he found out that his control on the signature device then he will still be responsible for the damages that were caused because of the use of his signature without his permission.

**Paragraph 4** This paragraph determines that a certified electronic signature is regarded as being a secured one. This means that a certified electronic signature will be regarded as having evidential status due to the fact that it will be considered secured.
Paragraph 5 This paragraph grants the court the authority to accept an electronic certificate that was issued by the Certification Authority. In discussions about the bill of law, different companies that hope to become Certification Authorities demanded that this clause be added because without it there is no actual advantage to the use of the services of a Certification Authority provider and the relevancy of the electronic certificate is negated.

Paragraph 6 This paragraph determines that an electronic document or message, which is signed with a secured electronic signature, will be considered original unless ruled differently by the Minister of Justice.

Paragraph 7 This paragraph refers to the responsibility of the signers. He is required by the law to assure that the signature device will not be compromised, and to be responsible for any damage related to the dependence on the signature. The law demands that the signer take appropriate means to guard the devices of electronic signature. The assumption is that the signer will best prevent any damage related to unauthorized use of his signature, and thus, through assigning liability to the signer, he is encouraged to take the necessary care. If the signature owner lost control of his device he must inform any party who is expected to rely upon his signature that he has lost control of the signature device.

This liability concerns the period during which the signature is controlled by the signer. The law doesn’t define clearly the steps that the signer must take and refers to the
reasonability factors according to law. This reference to the reasonability factor is necessary owing to the inability to foresee the total means of caution that are appropriate in cases using electronic signatures or other signature devices. In the regulations, which were composed for the bill of electronic signature, there are more specific rules.

In this paragraph, the signer was asked to inform any person who relied on his signature immediately when he realizes that his control of the signature device has been compromised. This liability is directed to the period of time after the control of the signer on his signature device was lost. In such a case, the signature owner must inform anyone that, in his knowledge, relies on his signature thereby acting to reduce the damage that could be caused to the other party. The law does not specify the means of informing, but it is possible to interpret this instruction as informing the other party in the most effective way, by which it is probable that the party will receive it. It is possible to interpret the probabilities in several ways: is it enough to pass a general message to the other parties through an electronic message board, or on certain Internet sites, or is it necessary to refer personally to any potential party through the e-mail or maybe through other media? It seems that courts will tend to interpret the rule strictly. Thus the responsibility is to use the most effective way that is reasonable to use under the circumstances. Where it is possible to locate e-mail addresses, and there is no problem which prevents referring to them in electronic mail, the signer will not fulfill his obligation if he informs the parties only through a general message in an electronic message board or a certain Internet site. Such messages are not certain to arrive personally to any party that relies on his signature.
If the signer has fulfilled all his legal obligations, he avoids the risk of being liable to any damage that may be caused because of any use of his signature device without his knowledge. If he did not fulfill his obligations, he is open to law suits because of any damage caused to the party that depended on his signature.

**Paragraph 8** This paragraph determines the special obligations that the signer of a certified electronic signature must fulfill. He must inform the Registered Authority of all the information he will be requesting regarding the Certification Authority. He also must inform the Registered Authority, in the event he loses control of the signature device, this is in addition to the signer’s informing any who are reliant on his signature. This enables the Certification Authority to revoke the electronic message, which was damaged, and to prevent future damage, which can be caused because of reliance on the violated electronic certificate.

If the signer fulfills these obligations, he will not be liable for damage caused following the unauthorized use of his signature. If the signer did not fulfill these obligations, it is possible to sue him for the damage of the reliance.

**Paragraph 9** This paragraph orders the rules of nomination of the Registered Authority. This paragraph enables the registration of Certification Authorities and the supervision of their activities. The Registered Authority, which is appointed by the Ministry of Justice, will manage a database of Certification Authorities that will be available to the public. The Registered Authority will also supervise the Certification Authorities fulfillment of the legal rules.
**Paragraph 11** This paragraph states the conditions for registering a Certification Authority. The Registered Authority will register a Certification Authority that fulfils the following conditions: an Israeli citizen or an organization which was incorporated in Israel, which has one of its purposes the management of a business as a Certification Authority. In some countries, the registration for Certification Authorities was limited only to governmental institutes or other financial organizations.

**Paragraph 11 (2)** In addition, the Certification Authority has to have reliable software and hardware systems that will allow reasonable protection from unlawful entry into a computer, and which provide a reasonable level of availability and credibility.

**Paragraph 11(3)** This paragraph determines the necessity to deposit a guarantee or to take out an insurance policy in order to assure compensation to any person who suffered damage because of an act of, or negligence by, the Certification Authority. Thus, the Certification Authority is liable. If it does not fulfill certain demands, it might be sued for the damages it caused. In order to assure that the party which suffered damages by the Certification Authority’s actions is compensated, the Certification Authority has to deposit a guarantee which is determined by the Justice Minister. The sum of the guarantee and its conditions depend on the scope of the Certification Authority activities, the type of certificates that it issues, and the limitations which are tied to the use of these certificates, as well as the level of their effect on the size of the expected damages. It seems that determining the sum of guarantee must take into consideration
the liability that the Certification Authority will carry as a result of the guarantee, and considering the scope of liability to which it is expected to be exposed The sum of insurance would depend on the electronic certificates that the Certification Authority issues or which it intends to issue.

**Paragraph 11(4)** The Certification Authority must have the ability to register the database according to the law of Privacy Protection (1981). The records of the Certification Authorities are considered a database according to the law of privacy protection and as such must register. This duty obliges the owner of the registered database to be liable for several other duties – including the duty to use the database only for the purpose for which it was established: to enable a person to review the information in the database which relates to him, to keep secret the information which will be gathered, and to secure the information which is already within the database.

**Paragraph 14** One of the main abilities of the Registered Authority is to stipulate the registration of the Certification Authority. If the register realizes that the Certification Authority does not fulfill the orders of the law, it is entitled, (after giving the right to the Certification Authority to explain its behavior) to detain its registration for a period of no longer than 30 days, or to revoke it totally from the records. After the registration has been detained, the register can lengthen the period of detention for an additional 30 days. If the Certification Authority does not change according to the demands of the Registered Authority by the given time, the Certification Authority will be deleted from the record. The Registered Authority’s decision is open to appeal in the district court for 45 days from the day that the Registered Authority decision was submitted.
**Paragraph 15 (a)** The Registered Authority has the ability to instruct a Certification Authority to change its software and hardware systems if the Registered Authority considers that it isn’t reliable enough or doesn’t protect sufficiently the public that uses its electronic signature.

**Paragraph 15 (b)** The Registered Authority is also allowed to change the sum of guarantee that he allotted the Certification Authority, in case a change occurs in the scope of the certification authority’s activities.

**Paragraph 17.** The Registered Authority can demand from any person related to the subject any information or document, which it needs that refers to the activities of the Certification Authority. The Register has the authority, if he is convinced it is necessary for the keeping of the law or for preventing a violation of his instructions, he may enter any place where the Certification Authority operates, search it and take any item. The Registered Authority can also authorize a state employee to perform this.

**Paragraph 18** The activity of a Certification Authority is to issue an electronic certificate that verifies electronic signatures. Parties who are not acquainted fear to depend on the other party’s presentation or its claim to be who it is. Thus, a Certification Authority is needed to verify the identity of the signer and to certify that a certain electronic signature is its signature.
Managing a database of certificates enables the party desirous of depending on an electronic certificate to call the database and review the details of the certificate. The database will also include a record of revoked electronic certificates, in order to ensure that it is impossible to rely upon them anymore. It is essential to use of reliable systems that issue reasonable protection against breaking into the computer and allot a reasonable level of availability and authenticity.

**Paragraph 19** In this paragraph there is a list of minimum conditions that must be part of an electronic certificate, such as the signer’s name and address, a certification about examination of the signature of the signer and other items, which are detailed within the paragraph.

**Paragraph 20** This paragraph determines when and how electronic certificates can be revoked. The Certification Authority will revoke electronic certificates for one of three reasons:

A. A demand of the certification owner, which will usually occur following the loss of control on his signature device. For example, where the signature device was lost or stolen, or if the password identifying the signer was exposed; or if he desires to stop the use of a certain signature device or to end an association with the Certification Authority.

B. When an item in the electronic certificate isn’t correct or that the purpose of the certificate has changed. The electronic certificate is based on information given and verified by the signer to the Certification
Authority. If the Certification Authority finds that the information given isn’t true or if there is an omission in the given certificate, it will revoke the certificate; or if the authenticity of the certificate was in any way damaged, such as by changes within it that awaken suspicion about the owner’s identity.

C. The death of the certificate owner or a liquidation of the organization.

The Certification Authority, must manage a database of the electronic certificates which it issued and later revoked. A party that needs to depend on an electronic certificate will examine the electronic certificate’s database, to determine whether the certificate, which is presented to him, is valid.

Revoking certificates – when the Certification Authority is obliged to revoke an electronic certificate and inform the owner of the certificate of its revocation and record it in the database of electronic certificates. In other words, the revocation must prevent future use of the electronic certificate.

**Paragraph 21** This paragraph determines the responsibility of the Certification Authority. If it does not fulfilled its obligation it will be exposed to liability of damages due to reliance on an electronic certificate which it issued.

For example:

a. Examining the details of the certificate. The law casts responsibility on the Certification Authority to check with ‘reasonable measures’ all the details in the application to issue electronic certificates.
The ‘reasonable measures’ can be interpreted by the function of the transactions or activities, which the signature device is supposed to be used for. In the electronic certificate, the Certification Authority defines the way that the signer’s signature was verified, and will also indicate the way that the other details that the signer gave were verified. The certificate shows the degree of reliability that can be referred to the details within it. It should also be noted that, in many cases, the Certification Authority offers several kinds of certificates, with limits of the sum of transactions that can be done through use of the certificate. For example, there are commercial companies that act as Certification Authority and offer a free electronic certificate for an experiential period and don’t verify the details of the signature owner. Such certificates are limited to transactions of 10,000 yen and the commercial company is not liable for transactions that were performed through reliance on the certificate with higher sums than recorded. The certifications present the verification that was done to the certificate and the relying party makes the choice whether to rely upon it or not.

b. In the paragraph 21, the law enables the certification factor to limit its liability to the kind of use that the electronic certificate can be put to, or to the sum of transactions for which it is possible to use the certificate. If the limitations were recorded within the certificate, the Certification Authority will not be liable for the damage caused following use that extends the recorded limitations. This enables the certification authority
to restrict the risk for which it is exposed through the use of the certificate and allow use of a variety of electronic certificates.

**Paragraph 22** In this paragraph the law recognizes the Certification Authority for electronic signatures outside of Israel, usually in countries with similar laws to the Israeli law.

**Summarization**

The law of electronic signature and the computer law are harbinger laws for the new technological era. Quite a few existing laws that are relevant to this subject will need to be adjusted to the new era.

For example, the need to change the laws of evidence, how to present electronic evidence which is composed of electric signals, or how to discover electronic information, when there is an order of documents presentation, or how to prevent the damage of evidence that is part of a software that can be deleted in minutes. Thus, a state, which doesn’t organize itself and change its laws according to the needs of technology, will find that its regular laws aren’t relevant anymore and belong to the past.

It would not be possible to implement existing laws on the new norms of computers and the Internet. If the appropriate legal changes are not made, the changes of technologies will still arrive to the courts, which will have to correlate themselves to the new factors without the backing of the law or other legal frameworks. Thus, where the legal world is not correlated to the new technologies there will exist an inability to legally use
the new technologies. For example, sending a document through a fax or e-mail will be problematic if the sender is not certain that he can convince a court of law that this document was sent and received. In most of the modern states today, including Israel, different laws are legislated that change the existing legal system and reorganize it to suite the technological age. The new laws are made through amending existing laws, changing the relevant paragraphs and amending them to the new era, or creating new complete bills of laws, such as the bill of computers and the bill of electronic signature; thereby open in an entire world of opportunities and enabling legal recognition of the technological world became part of our lives. These laws enable every person to enjoy that technological world and protect him from those who want to use it for illegal purposes.
Question 3

For the framework described above, to survey how the legal effect would be affected in case that the Algorithm is being compromised which is already used in electronic signatures or time stamps. Or Surveyor to report the schedule to which examination of a legal effect will be performed from now on.

The law of electronic signature 2001, paragraph 20, refers to what will happen when an electronic signature-cryptographic algorithm is compromised. The law determines that when the signature device of the certificate owner is no longer reliable, the Certification Authority must revoke the electronic certificate immediately. The law does not leave any option of doing something else such as regenerating the electronic document with an electronic signature. In this paragraph, the law proclaims all the cases where the electronic signature which has been compromised will be revoked. We will present two different cases:

A. The owner's request for cancellation of his certificate. The certificate owner could be the one harmed the most from a penetration into his electronic document, which he has signed. Thus, he can ask the Certification Authority to revoke the electronic certificate and the electronic signature as well. In this case the Certification Authority must immediately revoke the certificate, after verifying the identity of the certificate owner. The certificate owner can ask the Certification Authority to revoke his certificate for different reasons. For example when he suspects that his control of the signature device has been
disrupted due to loss or theft of the cryptographic device such as a “smart card”, or if his identifying password was exposed. Under such circumstances the signer will request the revocation of the electronic certificate in order to prevent the reliance of third parties on his signature. In addition, the certificate owner may request the revocation of the electronic certificate if he wants to continue using certain other signature devices.

B. Cancellation of a certificate by the Certification Authority Paragraph 20(2) the law determines that if there was any deficiency in the secured electronic signature of the signer, the Certificate Authority must revoke the electronic certificate.

Paragraph 21 (4) indicates that the Certificate Authority must revoke the electronic certificate if there is any deficiency which affects the certified electronic signature or its database, which can affect the integrity of the electronic certificate that it issued.

One of the main methods for discovering such deficiencies is through PKI (Public Key Infrastructure) technology which is an asymmetric cryptography. It is mostly used in order to verify that no changes were made in the signed document from the moment of its dispatch; thus, if the contents of the message have changed, the electronic certificate will be immediately revoked.

We must indicate that by Israeli law, it is not possible to hold the validity of the electronic signature. This is in contrast to other countries, where the certificate owner is able to ask to hold the electronic signature for a certain period of time.
Holding the validity of the electronic signature is done when the signer is afraid that the security of the signature device is at risk or when his control of the signature device is uncertain, but he may possibly regain the control and does not wish to revoke the signature immediately.

Liabilities
In the event that cryptographic algorithms are compromised, the liability could be on any party who is involved in the electronic document, depending upon their negligence or their contribution to the caused damage. At least one of the following three parties may be liable if an electronic algorithm is compromised:

a. The signer.
b. The party that relies on the signature
c. The Certification Authority
   a. **The signer:** Paragraph 7 in the law of electronic signature 2001, obligates the owner of the electronic signature device to take all the reasonable steps to protect his signature device and to prevent its unauthorized use. The assumption is that the owner is the only one who can prevent damage by protecting the signature device.
   The law of electronic signature does not determine special directives concerning the level of the signer’s responsibility to the harm caused by the reliance. Thus, the general Tort Law applies in such a suit. According to the general law of Tort, the signer is expected to be liable for any harm caused to the party that relies on the signature. In addition, where the
fault of the relying party is also a cause of the damage, the compensation rate will be reduced according to the estimation of the court as to what is justified and appropriate considering the level the relying party’s fault.

b. **The party that relies on the signature:** In order to prevent an exposure of the signer to legal claims because of unreasonable reliance, the UN international committee presented a set of uniform rules (February 2000) that clearly determine that a person cannot rely on an electronic signature in any way or measure that is not reasonable under the circumstances. A reliance which is not reasonable will not credit the relying party compensation. The reasonability of the reliance is determined following, among other things, the nature of the transaction, which was performed with the aid of the electronic signature, the knowledge that the relying party had about the existence of an electronic certificate, the information that the relying party had or had to have concerning the loss of control of signature means or their revocation as well as any agreements and commercial habits that the signer and the relying party had.

In determining whether reliance on the electronic signature is reasonable, the following questions will be checked:

1. The nature of the transaction that the electronic signature was intended to support.

2. Whether the relying party had taken appropriate steps to determine the reliability of the electronic signature.
3. Whether the relying party took steps to ascertain whether a
electronic certificate supported the electronic signature.

4. Whether the relying party knew, or ought to have known, that the
electronic signature device had been compromised or revoked.

5. Any agreement or course of dealing which the relying party had with
the signer, or any trade usage, which may be applicable.

6. Any other relevant factor.

c. The Certification Authority will be liable to any damage which was
caused due to the reliance on its electronic certificate, if it could be
proved that it did not take all the reasonable measures to fulfill its
obligations of the law of electronic signature. The law obliges the
Certification Authority to insure itself in order to compensate the people
who were harmed through its negligence.
Question 4

To survey if Israel government investigate any technical countermeasures and legal countermeasures for breaking any cryptographic system, and with what member it is investigated.

The subject of the breaking into cryptographic systems is an active subject within the Israeli Government, the parliament and other leaders of the Israeli market. Technical and legal devices are produced and created in an effort to prevent the breaking-into cryptographic systems.

The Ministries of Science and Technology, Justice, Treasury and Police are involved in this issue.

Following are the activities in each Ministry:

1. In the Ministry of Science and Technology there is a special committee which has as its purpose to map the threats on the civil infrastructure in Israel and to map the different technologies that can answer those threats. The committee doesn’t deal with operational subjects, but more in development and research technology. The members of the committee are among the leaders of academia, as well as public and government institutes. The first report of the committee will be submitted in 2005.

2. In the Ministry of Justice, this subject is mostly dealt with the legal conception of the subject of breaking into cryptographic systems.

   A. In the regulation for electronic signature (secured electronic signature, software and hardware2001), a cryptography software was chosen which its purpose the prevention of penetration or forgery of electronic
signatures. The regulation determines a strong and reliable software that the Certification Authorities must use when they provide electronic certificates, which includes private and public keys to parties that are interested in using an electronic signature. In other regulations related to the same law (recording of Certification Authorities and management 2001), The Justice Minister determines that the Certification Authority must record all unauthorized efforts to penetrate into the system in order to act against these factors.

B. Another law which is an example of the legal acts for preventing breaking into cryptographic systems is the Encryption Order that determines different instructions and rules to prevent breaking into cryptographic systems.

C. The Ministry of the Treasury established a general inter-organizational committee which includes representatives of all government ministries with the purpose of acting in the subject of software, including cryptographic technologies that relate to all government ministries. This committee publishes their recommendations to all ministries.

In every ministry there is a committee which deals with databases and each is in charge of the means to prevent penetrations to their own cryptographic systems. When this committee needs to buy any type of cryptographic software, the representative of the Ministry of the Treasury participates in this decision.

This perception enables an overall view of the quality of the cryptographic software that the government offices purchase, and helps
to prevent breaking into the cryptographic systems of the ministry.

During 2003 there were more than 1,000 break-in trails to governmental cryptographic systems and only 8 minor cases succeeded in penetrating into systems. This shows that the government succeeded in protecting its cryptographic software.

D. The Ministry of Police is an important factor in the efforts of prevention of breaking into all civil cryptographic systems. The police use different sophisticated software and other devices to try to locate people who attempt to break into cryptographic systems. The Ministry of Police refuses to reveal the technology which helps them in their duty.

E. The Ministry of Defense, which is in charge of the performance of the Cryptographic Order, uses these instructions in order to prevent break-ins cryptographic systems. The Cryptographic Order authorizes the supervisor not to allow the import or the export of cryptographic systems that are at risk from a break-in that may harm Israeli state interests. This office established a committee in the Ministry General Director’s office that advises the General Director on the subject. The role of the Defense Ministry is not only to protect cryptographic software but also to use the cryptographic system in order to balance other considerations, such as commercial considerations or rules of privacy protection and public freedom.

The Israeli parliament raised the issue of braking into cryptographic systems in July 2004 and ordered a hearing of different representatives from the government, the
industry and academia in order to decide how the government offices should prepare, to defend themselves from one of the most threatening subjects of the computerized world: penetration into cryptographic systems.

The participants reported their activities and the need to strengthen Israeli activity in the field of preventing break-ins to cryptographic systems. The reports showed that most institutes already use security systems in order to prevent breaking into cryptographic systems. Most of the software that is used is developed and produced in Israel.

The conclusion of the hearing was that a special civil authority must be established in order to coordinate all the information connected with break-in trails into cryptographic systems, such as: who breaks-in, what is the character of the break-in trails, the number of break-ins, and the sophistication or lack of it. Another possibility that was raised in the hearing is the need to establish an international Internet forum where different representatives of the government, the banks and other relevant institutes will discuss different subjects related the to Internet, especially the subject of breaking into cryptographic systems.

In 1997, the Israeli Government established a central body by the name ‘Tehila’ to take care of preventing penetration into data security of government systems and for the governmental infrastructure for the Internet era.

Tehila is the central body that provides Government Ministries and Institutions with highly secure Internet services. In this way the dangers associated with connecting these networks to the Internet is significantly reduced.
The Tehila project began in 1997, to answer the growing need of Government Ministries to be connected to the Internet, in order to:

- Provide services and information
- Make use of Internet resources
- Communicate via email with people both in Israel and worldwide.

The Tehila project aims to provide a solution to the risks associated with exposing the Government network, in terms of information security, by connecting Government Ministries with appropriate security and control measures.

Tehila's main mission is to provide two main services:

1. Secure access to Internet services for Government users. Users receive a service package that meets with the specific information security requirements.
2. Hosting of Government websites that provide information and services to the public, while using information security mechanisms to protect the data.

The goals of the Tehila project

1. To provide Government users with access to basic Internet services, while minimizing the information security risk to Government office computer systems.
2. To make Internet services available to a large number of workers who require them and are unable to access them at their desks due to information security concerns.

3. To build a secure platform upon which Government applications and data can appear on the Internet.

4. To accelerate the entry of Government offices to the Internet world, by creating an inexpensive and readily available infrastructure for creating websites.

5. To provide solutions to the problems encountered when entering the Internet world with the goal of distributing information to citizens.

6. To conserve resources for Government offices that are required to setup Internet infrastructures including: hardware, software and communication infrastructures.

Tehila Server Farm

Tehila’s Server Farm is located in the Government complex in Jerusalem. It hosts websites of Government offices and bodies that invest a great deal of effort in exposing information and online services as part of the eGovernment revolution.

A highly trained, world-class staff maintains the Server Farm 24-hours-a-day, 7 days a week, with maximum security. Entrance to the Server Farm is permitted only to authorized personnel and is departmentalized using advanced protection methods, including retinal scans, use of smart cards and more.

Hosting possibilities vary – from server and/or database hosting on the Tehila hosts to
hosting of independent servers in the Server Farm, while taking advantage of the security and maintenance Tehila provides.

The Communications Center infrastructure is protected using various means: flood warning equipment, fire detection and extinguishing systems, and air conditioning systems, which maintain optimal temperature conditions.

The Server Farm is also protected by a UPS (Uninterruptible Power Supply) system that guarantees that the system will remain available even during emergency situations.

The Server Farm is continually backed-up. Back-ups are stored at an external location.

Tehila uses a variety of resources to maintain its information security goals – beginning with a staff of Information and Communication Security experts and continuing with a variety of products and technologies of world-leading companies. Security systems at Tehila stopped approximately 250 attacks on Communications Systems and components of protected Government networks in 2002.

- Approximately 45 formal letters of complaint were sent daily.
- 90,000 attempted attacks were seen, with 14,000 of them considered of high quality.
• Tehila’s automatic testing systems tested approximately 6.7 million objects in
surfing traffic from within government offices – almost 2.5 billion objects.
Approximately 19,000 were tainted with harmful software.

• Tehila’s mail servers process an average of 85,000 messages daily – about 30GB
of data. On days with email attacks, there may be as many as 550,000 messages.
Each day approximately 100 virus attacks and attacks of other harmful software
are avoided. On days with email attacks, up to 80,000 harmful messages are
received.
Question 5

To survey in Israel, how to perform the research-and-development activities about the cryptographic technology and its application systems used in government organizations excepting the Department of Defense and the Ministry of Foreign Affairs.

In Israel the activity on the subject of development and research of cryptographic systems designated for government offices is coordinated by the Treasury office. The office established a committee by the name Mercava that includes representatives of all the ministries. The committee is responsible for research and development data for the following subjects:

A. A central database in the logistic, financial and manpower.
B. Inter-departmental cooperation to determine the structure and implementation of the system.
C. Building central interfaces for input and output media into the governmental databases.
D. Establishing a central governmental communication system (intranet) for the implementation of the committee’s decisions.
E. Implementing the law of electronic signature which enables the performance of most public activities with the government on-line.

Another committee within the Treasury office called ‘Tamar’ deals with the prevention of breaking into cryptographic systems from the following aspects:
A. The crystallization of a perception that will enable the establishment of electronic governmental activities.

B. Approach to personal databases.

C. Improvement of the level of information security within government offices.

D. Cooperation with the American and European markets on the subject of electronic identification and inter-governmental activities.

E. Method of the communication between the citizens and the government through cryptographic systems.

F. The committee deals with other subjects related to cryptography, which are shared by the different government ministries, and is responsible for the direct research and development of this subject, which is connected to all the governmental offices.

Besides these two central committees, an internal authority exists in each government office that takes care of cryptographic subjects related to its office's needs. This internal committee, which operates in every office, decides which cryptographic systems to use, and whether certain cryptographic software be used or developed internally or through a mediating company. Sometimes the committee will enlist software specialists for the development of a certain system to a certain project.

The government ministries are not subjugated to the Cryptographic Order.
Question 6

To survey if Israel government validate the cryptographic product used in government organizations excepting the Department of Defense and the Ministry of Foreign Affairs. When the cryptographic product is validated, Surveyor to report if there are a requirement and evaluation Criteria, if it is opened to the vendors. If opened to the public, Surveyor to report the contents.

The government authorizes cryptographic systems, through the Treasury and Justice Ministries. Details of committees that are central to all government ministries were presented in Question no. 5. and also in paragraph 23 of the Electronic signature law. The Minister of Justice set the conditions for the transfer of electronic messages with electronic signature to the government and from the government.

An additional activity of the government is a special project established in 1997 that advances the Internet, and its services through public activities (detailed in answer number 4).

When a cryptographic product is validated, the requirements of the level of cryptography depend upon the contents and the importance of the material. There are cases where the protection that is given to the cryptographic material used is as much as ten protective layers. It is not possible to find out what these protective layers are, what criteria is used to evaluate and determine the strength of cryptography in any document.

The different government ministries purchase cryptographic systems in correlation to
their needs, if they cannot develop their own systems. When a cryptographic system is purchased, it necessitates the decision of an inter-departmental committee with a Treasury office representative, that determines which software to buy and the level of strength needed.

Often the cryptographic systems that are purchased by the government offices go through changes and are adjusted to the specific needs of the office or the needs of material.

The material concerning the software systems that are purchased or the criteria by which they are chosen is not open to the public.

This information was received form people who deal with the database in the different government offices.