

Al-Wakaye Al-Mesreya / Government Bulletin - Issue No. 115 (Supplement)
Dated 25 May 2005

Ministry of Communications And Information Technology
Decree No. 109 Of The Year 2005
Dated 15/5/2005
Issuing The
Executive directive
Of The
Electronic Signature Law
And Establishing The Information
Technology Industry Development Agency (ITIDA)

The Minister of Communications and Information Technology,
Following thorough review of the Constitution;
The Civil Code;
The Trade Law;
Law No. 13 of the year 1968 on Civil and Commercial Procedure;
Law No. 25 of the year 1968 concerning evidence in civil and commercial matters;
Law No. 82 of the year 2002 on protection of intellectual property rights;
Law No. 10 of the year 2003 on regulation of telecommunications;
Law No. 15 of the year 2004 regulating Electronic Signature and establishing the Information Technology Industry Development Agency;
And presidential decree No. 201 of the year 2004 forming the cabinet of ministers,

DECREES THE FOLLOWING

Article : 1

The provisions of the attached executive directive of law No. 15 of the year 2004 regulating Electronic Signature and establishing the Information Technology Industry Development Agency shall come into force.

Article : 2

The present decree shall be published in Al-Wakaye Al-Mesreya / Government Bulletin, and shall come into force effective the day following the date of its publication.

**Minister Of Communications
And Information Technology
Dr. Tarek Kamel**

Article : 1

In applying the provisions of the present directive , the following terms shall denote the meanings indicated next to each of them :

- 1- Electronic Signature (E-signature):**
What is put on an e-document and takes the shape of letters, numbers, characters, signs or others, besides having an exclusive feature that allows identifying the signing person and distinguishes him from others.
- 2- Electronic Writing (E-writing):**
All letters, numbers, characters or any other signs that are fixed on an electronic, digital, or light support or any other similar method and provide a perceptible connotation.
- 3- Electronic Document (E-document):**
A data message comprising information originated, merged, stored, sent or received, wholly or partially, by an electronic, digital, or light method, or any other similar means.
- 4- Electronic medium (e-medium):**
E-signature creation device(s), or systems.
- 5- Signer:**
A person possessing the signature creation data, who signs for himself, for whoever delegates him, or for the one he legally represents.
- 6- Certificate Service Provider (CSP):**
The entities authorized to issue the digital certificate and offer services related to the electronic signature.
- 7- Digital Certificate:**
The certificate issued from the entity authorized for providing certificate services, and proves the correlation between the signer and the signature creation data.
- 8- Electronic Signature Creation Data:**
The exclusive elements concerning the signer and distinguishing him from others, including in particular his public/private (cryptographic) keys that are used in creating the electronic signature.

9- Cryptography

A technical algorithm using special keys for treating and transforming the data and information electronically read in a way that prevents extracting these data and information except by using the decrypting key(s).

10- The Public and Private Keys Technology (Known by the name Public Key Infrastructure):

A system allowing every natural or juridical person to possess two separate keys, one of them is public and electronically available, and the second is private and to be kept with the person as highly confidential.

11- The Public Key:

An electronic tool available to everybody created by means of a special mathematical operation and used in checking the identity of the signer to the electronic document and in ensuring the validity and security of the original electronic document content.

12- The Private Key:

An electronic tool pertaining to its holder, created by means of a special mathematical operation, and used in putting the electronic signature on the electronic documents. It shall be preserved on an secured smart card.

13- Root Key:

An electronic tool established by means of a special mathematical operation and used by the electronic ratification entities for creating the digital certificates and the electronic signature creation data.

14- Electronic Support :

A physical medium for keeping and circulating the electronic writing, including the compact disks (CDs), light disks, magnetized disks, the electronic memory or any other similar medium.

15- Smart Card:

A secured electronic medium used in the process of creating and fixing the electronic signature on the electronic document. It contains an electronic chip having an electronic processor, storage elements, and programs for operation. This definition comprises the smart cards, the smart tokens or what is similar to them in accomplishing the

required tasks with the technical criteria defined in the present directive .

16- The Computer:

An electronic set capable of storing, treating, analyzing and retrieving the data and information electronically.

17- Computer Program:

A set of commands and directives expressed by any language, symbol or sign, and taking any form. It can be used directly or indirectly in a computer for performing a task or achieving a result, whether these commands and directives are in their original form or in any other form of appearance through the computer.

18- The System of Forming the Electronic Signature Creation Data:

A set of interconnected and integral elements including electronic media and computer programs by which the data for creating the electronic signature is formed using the root key.

19- The System of Originating the Electronic Signature:

A group of interconnected and integral elements including electronic media and computer programs by which the electronic document is electronically signed using the of the electronic signature creation data and the digital certificate. Also, the electronically signed document is placed and fixed by them on an electronic support.

20- Certificate of Examining the E-signature Creation Data:

A certificate issued by the Agency with the result of examining and checking the validity of the e-signature creation data.

21- E-signature Examination Certificate:

A certificate issued by the Agency with the result of its examination of the validity and security of the E-signature.

22- Certificate of Approval of the Foreign Certificate service providers Entities:

Certificate issued by the Agency approving the foreign certificate service provider entities and the similar digital certificates issued by these entities within the Arab Republic of Egypt.

23- The Agency:

Information Technology Industry Development Agency (ITIDA).

24- The Concerned Ministry:

The ministry concerned with communications and information technology.

25- The Concerned Minister:

The minister concerned with communications and information technology.

26- The Law:

Law No. 15 for the year 2004 regulating the Electronic Signature and establishing the Information Technology Industry Development Agency.

Article : 2

The system of forming the e-signature creation data shall be secured once it fulfills the following:

- a) The exclusive nature of the e-signature creation data;
- b) The secrecy of the e-signature creation data;
- c) The non-possibility of deducing the e-signature creation data;
- d) Protecting the e-signature against forgery, imitation, perversion, artificiality or any other forms of manipulation, or against the possibility of being created by other than the signer;
- e) Non-committing any damage to the content or meaning of the e-document required to be signed;
- f) This system shall not prevent the signer from fully learning all about the content of the e-document before signing it.

Article : 3

The secured system of forming the e-signature creation data shall comprise the necessary technical and technological controls, particularly the following:

- a) The system shall be based on the general and private keys code technique and the root key of the authorized entity, as issued for it by the Agency. All this shall be according to the technical and technological criteria referred to in clause-A of the technical and technological annex of the present directive ;
- b) The technique used in creating the root keys of the certificates service provider entities shall use code keys with lengths not less than 2048 electronic bits;
- c) The hardware security modules used shall be approved according the technical and technological controls referred to in clause-B of the technical annex of the present directive ;
- d) Non-replicable smart cards protected by a secret code shall be used containing exclusive elements of the signer, which are the e-signature creation data and the digital certificate. The specifications and systems of the smart cards shall be determined according to the technical criteria indicated in clause(C) of the technical annex of the present directive ;
- e) The system shall ensure for all dealing parties the availability of the data pertaining to the verification of the validity of the e-signature and its linkage with the signer exclusively. It shall also ensure the process of immediate inclusion and instant availability of the lists of suspended or canceled certificates upon realizing the existence of reasons necessitating the suspension of the certificate, providing such verification shall take place within a period defined and known to the users according to the rules and controls set by the board of the Agency.

Article : 4

The board of the Agency may set other systems and rules for the system of forming the e-signature creation data to keep abreast of technical developments.

Article : 5

The Agency shall be the higher Root CA in the Arab Republic of Egypt. It shall issue the root keys concerning the entities authorized to issue digital certificates.

The Agency, before granting a license for exercising the activity of issuing digital certificates, shall ascertain that the system of forming the e-signature creation data with the authorized entity is secured according to article-2 and comprising the technical controls, as well as the systems and rules indicated in articles Nos. (3,4).

The system, after granting the license and throughout its validity period, shall be considered secured and effective unless otherwise established.

Article : 6

The Agency, upon the request of any concerned party, shall provide the service of examining and verifying the validity of the e-signature creation data against a charge the rates of which shall be defined by the board of the Agency. The Agency may entrust to third parties the task of providing this service under its supervision. In all cases, the Agency shall issue the e-signature creation data examination certificate.

Article : 7

The Agency, upon the request of any concerned part, shall provide the service of examining the e-signature against a charge the rates of which shall be defined by the board of the Agency. Toward providing that service, the Agency shall ascertain the following:

- a) The validity of the digital certificate and its conformity with the e-signature creation data.
- b) The possibility of determining the content of the signed electronic document accurately.

- c) Easiness of knowing the person of the signer, whether in case of using his original name or an alias or assumed name.

The Agency may entrust to third parties the task of providing this service under its supervision. In all cases, the Agency shall issue the e-signature examination certificate.

Article : 8

Subject to the conditions prescribed in the Law, the proof conclusiveness prescribed for the electronic writing, and the official or non-official electronic documents shall be established for their creator, if the following technical controls are fulfilled:

- a) Determining the time and date of creating the electronic writing or the official or non-official electronic documents shall be technically available. Such availability shall take place through an independent electronic save system, which is not subject to control by the creator of that writing or these documents or by the party concerned with them.
- b) Determining the source of creating the electronic writing or the official or non-official electronic documents, and the degree of their creator's control on that source and on the media used in creating them shall be technically available.
- c) In case of creating and issuing the electronic writing or official or non-official electronic documents without human intervention, partially or wholly, their conclusiveness shall be established once it is possible to ascertain the time and date of their creation, and if such writing or documents have not been tampered with.

Article : 9

The electronic signature connection exclusively with its signer shall be ascertained technically once this signature is based on an electronic signature creation data formation system secured as prescribed in articles Nos. (2, 3, 4) of this directive , with one of the following two cases fulfilled:

- a) This signature shall be connected with an approved and valid digital certificate issued by an authorized or accredited certificate service provider entity;
- b) Ascertaining the validity of the e-signature according to article-7 of the present directive.

Article : 10

The signer's exclusive control on the electronic medium used in the process of fixing the electronic signature shall be technically ascertained through the signer's possession of the private key save tool, comprising the secured smart card and the secret code linked to it.

Article : 11

Subject to the provisions prescribed in articles Nos. (2,3,4) of the present directive, any amendment or change in the data of the electronically signed e-document shall be technically revealed by using the general and private keys technique, and by matching the digital certificate and the electronic signature creation data with the original of that certificate and these data, or by any similar method.

Article : 12

The applicant for a license to issue the digital certificates shall fulfill the following requirements:

- A) A system for securing the information and protecting the data and its confidentiality with a protection level not lower than the level prescribed in the criteria and rules referred to in clause-D of the technical annex of the present directive;
- B) A guidebook comprising the following:
 - 1- Issuance of the digital certificates;
 - 2- Keys management;
 - 3- Internal works management;
 - 4- Insurance and disasters management.

According to the technical criteria prescribed in clause-E of the technical annex of the present directive;

- C) A system for the formation of e-signature creation data, secured according to the technical controls prescribed in articles Nos. (2,3,4) of the present directive;
- D) A system for determining the date and time of issuing the certificates, discontinuing, suspending, re-operating or canceling them;
- E) A system for verifying the persons to whom the digital certificates are issued and examining their distinguishing characteristics;
- F) Experienced specialists holding the necessary qualifications for performing the licensed services;
- G) A system for storing the data of the e-signature creation data and the digital certificates throughout the period determined by the Agency in the license and according to the kind of the issued certificate, with the exception of the private keys issued by it to the signer, which shall not be stored except upon the request of the signer and by virtue of an independent contract to be concluded between the licensee and the signer and according to the technical rules of storing these keys as shall be set by the board of the Agency;
- H) A system for maintaining full confidentiality of the works connected with the licensed services and the data concerning the customers;
- I) A system for discontinuing the certificate in case of proving the existence of one of the following situations:
 - 1. Tampering with the data of the certificate or expiry of its validity period;
 - 2. Stealing or losing the private key or the smart card, or upon suspecting the occurrence of such stealing or losing;
 - 3. Non-observance by the person to whom the digital certificate is issued, of the articles of the contract concluded with the licensee.

The system of discontinuing the certificates shall be according to the rules and controls to be set by the board of the Agency;

- J) A system enabling and facilitating the Agency's verification of the validity of the e-signature creation data, particularly within the context of the inspection and verification works on part of the Agency.

Article : 13

In all cases, the licensee shall not conclude any contract with the customers expect following the Agency's approval of the form of that contract according to the rules and controls to be set by the board of the Agency in this respect for securing the rights of the concerned parties.

Article : 14

The applicant requesting the license for issuing digital certificates shall submit the guarantees and security deposits to be determined by the board of the Agency for covering any damages or risks connected with the concerned parties, in case of terminating the license for any reason, or for covering any violation thereby of his obligations as mentioned in the license.

Article : 15

The following procedures shall be followed for obtaining the license authorizing the issue of digital certificates:

- a) Submitting the request on the forms to be provided by the Agency in this respect, accompanied by the data and documents establishing the fulfillment of the conditions and provisions prescribed in articles nos. (3, 4, 12, 14) of the present directive;
- b) The Agency, after receiving all required documents and data, according to item-A, from the license applicant, shall examine them and check their validity. The Agency shall decide the application for obtaining the license within a period not exceeding sixty days from the date the applicant fulfills all that the Agency requires from him, unless the Agency notifies him of extending this period. In case this period lapses without issuing the license, the application shall be considered refused;

- c) The board of the Agency shall determine the charge for issuing and renewing the license and the rules and procedures of its collection. The licensee shall settle this charge upon being granted the license;
- d) The Agency shall grant the license according to the procedures and guarantees prescribed in the law and the present directive and also according to the rules to be set by the board of the Agency in this respect.

Article : 16

The Agency shall inspect the licensee entities for examining the degree of their compliance with the license.

Article : 17

The licensee's obligations shall be determined in the license according to the Law and the present directive as well as the Agency's board decisions to be issued in this respect.

Article : 18

A special table shall be established at the Agency for recording the licensed entities. Each entity shall be given a serial number and the kind of the license granted to the licensee shall be defined in such table. It shall comprise data about this entity, its capital, its board members, the managers therein, its branches and its offices, and such other data as shall be determined by the board of the Agency.

Article : 19

The Agency shall be the entity concerned with offering the technical consultation and expertise works concerning the disputes arising between the parties concerned with electronic signature activities, electronic dealings and information technology, providing coordination shall take place between the concerned entities with regard to the expertise works.

Article : 20

The forms of digital certificates as issued by the licensee shall comprise the following data, in a manner compatible with the criteria determined in item-A of the technical annex:

- 1- Evidence of the validity of this certificate for use in electronic signature;
- 2- Subject matter of the license issued for the licensee indicating its scope, its number, date of its issue and its validity period;
- 3- Name and address of the entity issuing the certificate, its head office, legal entity and the country to which it belongs, if any;
- 4- The signer's original name or his assumed or alias name, in case of using any of them;
- 5- The signer's quality;
- 6- The certificate holder's public key that corresponds to his private key;
- 7- Date of starting the validity of the certificate and its expiry date;
- 8- Serial number of the certificate;
- 9- The electronic signature of the entity issuing the certificate;
- 10- The website appropriated for the list of suspended or canceled certificates.

The certificate may comprise any of the following data whenever necessary :

- 1- Indication of the signer's specialization and the purpose for which the certificate is used;
- 2- Limit of the amount of dealings allowed by the certificate;
- 3- Fields of using the certificate.

Article : 21

The Agency may accredit the foreign entities concerned with issuing the digital certificates in one of the following cases:

- a) The foreign entity's fulfillment of the rules and conditions specified in the present directive with regard to the entities authorized by the Agency to exercise the activity of issuing the digital certificates;
- b) Existence of an agent for the foreign entity in the Arab Republic of Egypt being authorized by the Agency to issue Digital certificate certificates, and having all constituents required for dealing with the digital certificates along with warranting that entity regarding the digital certificates issued by it as well as the conditions and guarantees required to be fulfilled;
- c) The foreign entity shall be among the entities which the Arab Republic of Egypt has agreed to accredit, by virtue of an international convention applicable therein, considering it a foreign entity concerned with issuing the digital certificates;
- d) The foreign entity shall be among the entities approved or authorized by the licensing authority in its respective country to issue digital certificates, providing an agreement in this regard shall be concluded between the foreign licensing entity and the Agency.

Approval of these foreign entities shall be upon a request submitted by them or by the concerned parties on the forms to be provided by the Agency. The Agency, in the cases referred to in items (A, C, D) may also have the right of approving these entities by itself.

In case of submitting an approval request, the Agency, after receiving the required documents and data, shall examine them and verify their validity, and the board of the Agency shall decide the approval request within a period not exceeding sixty days from the date the foreign entity fulfills all requirements of the Agency. In case this period lapses without issuing the approval, the request shall be considered rejected unless the Agency notifies the requesting entity of extending this period.

The decision of approving the foreign entity shall be issued by the board of the Agency after settlement of the charge to be determined by the board for such approval. The approval period and its renewal conditions shall be determined in the decision. The Agency shall

always, by virtue of a substantiated decision, have the right to cancel or suspend the approval.

Article : 22

The accredited foreign entities may request the Agency to approve the kinds or categories of the digital certificates issued by them, which shall be according to the rules and controls to be set by the board of the Agency in this respect, and also to determine the charge for approving these certificates. The board of the Agency, upon approving the kinds and categories of the foreign certificates, shall determine the digital certificates equivalent to them, which are issued by the authorized entities in the Arab Republic of Egypt.

Article : 23

Subject to the penalties prescribed in article-23 of the Law, the licensee shall abide by all provisions of the license issued to him by the Agency. In case the licensee violates any of them or discontinues exercising his licensed activity, or in case of merger of the licensee's establishments into another entity or assigning the license to third parties without obtaining the Agency's prior approval of any of the said actions, the Agency, by a substantiated decision, may then cancel the license or suspend it pending rectification or correction.

The Agency, in both cases of cancellation or suspension, may take the appropriate measures in this respect for protecting the rights of concerned parties.

Article : 24

Subject to the provisions of the Law, whoever has been exercising the activity of digital certificates, before the effective date of the law, shall adapt his state of affairs to the law by submitting an application within two months from the date of issuing the present directive on the form to be provided by the Agency for the purpose, accompanied by the requirements of the Agency. The Agency shall decide the application within three months from the date the applicant fulfills all the Agency's requirements therefrom.

Whoever refrains from adapting his state of affairs according to the foregoing shall be considered to be exercising that activity without license, in which case the Agency may take all necessary measures for suspending the activity.

Technical Annex

The technical standards prescribed in the present annex shall be enforced, and any subsequent amendments or additions to be determined by the board of the Agency shall be published in Al-Wakaye Al-Mesreya / Government Bulletin after their approval by the concerned minister.

Clause (A)

PKI Technology

- The profiles for PKI operational management protocols must be based on PKIX (X.509-based PKI).
- The profile for Qualified Certificates must be based on X.509 (RFC 3739).
- At least one of the following algorithms must be deployed :
 - Symmetric algorithms (AES, [n]DES, CAST5, BLOWFISH, TWOFISH, IDEA etc.)
 - Asymmetric algorithms (DSA, RSA, El Gamal, RC [n] etc.)
 - Hash algorithms (MD5, SHA-1 224 etc.)
- Minimum RSA/DSA key lengths must be at least 1024 bits until the end of 2006. Increasing the length to 2048 bits is recommended with a view to guaranteeing long-term security levels.
- A baseline Certificate Policy for service providers issuing qualified certificates should be written according to the IETF (Internet Engineering Task Force) PKIX framework RFC 3647.

Clause (B)

Hardware Security Modules

- For e-signature creation and verification product and in trustworthy hardware devices used as secure signature creation devices, it is required to have concurrent acceptance and usage of FIPS 140-1 level 3 or higher, or equivalent standard such as suitable protection profile based on common criteria (ISO 15408).

Clause (C)

Smart Cards

- Smart Cards able to store private e-signature keys for a card holder without delivering the key to the outside world. Therefore, the calculation of the signature algorithm as well as its storage is performed in a highly secure environment inside a smart card. Thus, it is required to have smart cards (Reader / Readerless / contactless) which use the most advanced security standard available in the market.

Security evaluation ITSEC E4 or NIST FIPS PUB 140-1 level 2 or higher	
X . 509v3 certificates	ISO 7816
Cryptographic algorithm must include RSA,SHA-1	
Microsoft PC/SC	Recommended CAPI Microsoft Cryptographic
Recommended: PKCS #11 (interface)	Recommended PKCS #15 (syntax standard)

Clause (D)

Security Standards

- General Security management codes of practice, such as BS 7799-2 (British Standards, Information Security Management Systems Specification with guidance for use) and its guidance ISO/IEC17799 (recommended), or equivalent standard.

Clause (E)

Operation Standards

- Recommended : ETSI (The European Telecommunications Standards Institute) TS 101 456 V1.2.1 (2002-04) Policy requirements for certification authorities issuing qualified certificates, specifically Chapter 7 which covers the following parts:

- Certification practice statement.
- Key management life cycle.
- Certificate management life cycle.
- CSP management and operation or equivalent standard.