We, President of the State of Palestine
Chairman of the Executive Committee of the Palestine Liberation Organisation
President of the Palestinian National Authority

Having taken cognizance of the 2003 Amended Basic Law and amendments thereof,
Law No. 2 of 1997 on the Palestinian Monetary Authority,
The Banking Law no. (9) of 2010,
The Securities Law No. (12) of 2004,
The Evidence Act No. (4) of 2001,
The Commercial Law No. 12 of 1966,
Based on the authorities conferred upon us,
To serve the public interest,
In the name of the Arab Palestinian people,

Have issued the following law:

**Chapter One**

**Article 1**

**Definitions**

The following terms and expressions shall have the meanings indicated below, unless the context indicates otherwise:

**Ministry**: Ministry of Telecommunications and Information Technology
**Minister:** Minister of Telecommunications and Information Technology

**Council of Ministers:** Council of Ministers of the Palestinian National Authority

**Authority:** General Authority of Electronic Certification

**Transactions:** An action or a set of actions that take place between two or more parties to establish commitments on one party or mutual commitments among more than one party

**Electronic Transactions:** transactions concluded or performed, in whole or in part, through electronic means

**Electronic Data Exchange:** transfer of information from one person to another by electronic means

**Electronic Means:** Any modern technology-related means having electrical, digital, magnetic, wireless, optical, electromagnetic, photonic or any suchlike capabilities used in exchanging and storing information

**Electronic Data:** Any data which are electronically represented or coded whether in the form text, code, sound, graphics or otherwise

**Electronic Record:** A set of information which form together a description of a situation related to a person or a thing, that is established, sent, received or stored by electronic means

**Electronic Medium:** An electronic means or programme used to automatically
carry out a particular action

**Electronic Contract**: An agreement concluded by electronic means or media

**Electronic Signature**: Electronic data that are added to, incorporated in or associated with an electronic transaction, and have a nature that enables the identification of the person who signed them and distinguishes the signatory from others in order to agree to the content of the transaction

**Information Processing System**: The electronic system used to establish, send, receive, or store data messages or process them in any other manner

**Data Message**: Electronic information sent or received by electronic means

**Electronic Instrument**: A negotiable commercial bill

**Person**: A natural or legal person

**Signatory**: A person who holds an Electronic Signature Creation Device used to sign an electronic transaction

**Signature Creation Device**: A programme used to establish an electronic signature on transaction

**Sender**: A person who, in person or on whose behalf, originates or sends a data message before the addressee receives and stores it

**Addressee**: A person to whom the data message was sent
**Authentication Procedures**: Procedures meant to verify that an electronic signature is that of the signatory himself and that the content of the message has not been altered since its creation.

**Illegal Record**: Any financial record incurred by the customer as a result of a data message sent on his behalf unbeknownst to him, without him agreeing to it, or without his authorization.

**Encryption**: The process of converting electronic data into such a form that they are impossible to read and understand unless they are converted back into their original form.

**Certificate**: An electronic attestation certificate issued by an authority or a body authorized by it in order to establish the link between the signatory and the electronic signature data.
General Provisions

Article 2

Objects of the Law

The objects of law are as follows:
1- To facilitate and regulate electronic transactions by reliable electronic communications or records;
2- To eliminate barriers or challenges to electronic transactions arising from uncertainties over writing and signature requirements, and promote the development of the legal infrastructure necessary to implement secure electronic transactions and subsequent amendments;
3- Minimize the likelihood of forged electronic communications, alteration of communications and fraud in electronic transactions;
4- Establish uniform legal rules, regulations and standards for the authentication and validity of electronic communications and records;
5- Promote the growth of electronic commerce and other transactions on the national and international levels through the use of electronic signatures.

Article 3

Scope of Application

The provisions of this Law apply to the following:
1- Electronic transactions, records and signatures as well any electronic Data Message;
2- Electronic transactions used by any government department, official institution or private entities, in whole or in part.
Article 4
The following transactions shall be excluded from the scope of this Law:
1- Transactions and issues relating to personal status law such as marriage, divorce and wills;
2- Transactions to dispose of immovable property, including related proxies and title deeds and the establishment of rights in rem over them, with the exception of lease contracts relating to these matters.

Article 5
Without prejudice to the provisions specified in the above article, the provisions of this Law may apply to the above-mentioned transactions if relevant laws so permit.

Article 6
1- The provisions of this Law apply to transactions between the parties who agree to conduct their transactions by electronic means unless it is expressly stipulated otherwise.
2- Without prejudice to the provisions of paragraph (1), an agreement between particular parties to conduct specific transactions by electronic means shall not necessarily require them to conduct other transactions by those means.

Article 7
With regard to jurisdiction, the very provisions that apply to the electronic transactions and signatures shall apply to written transactions.
Chapter Two
Legal Consequences of Electronic Transactions

Article 8
1 - The electronic transactions and signatures shall have legal effect and shall be as valid and enforceable as written documents under the provisions of the legislation in force in terms of binding the parties thereto or their validity to serve as evidence.  
2- A paper copy of the official Electronic Data Message shall be binding on all the parties as long as it is equivalent to the original of the Data Message.

Article 9
1 - For the purpose of contracting, an offer and the acceptance of an offer may be expressed by electronic communications. That expression shall be binding on all the parties where it is done in accordance with the provisions of this Law.
2 - Notwithstanding the provisions of paragraph (1), the parties to the contract may agree that the contract is valid and enforceable if willingness is expressed in part through the Data Message.

Article 10
Unless otherwise agreed by the parties to the contract, an offer is deemed:
1- To be given through the Data Message upon its dispatch or at the time when it enters an Information System outside the control of the originator of the message;
2- To be received by the addressee at the time when the Data Message enters an Information System the parties to the contract agreed to use or enters the addressee’s information system.
Article 11

Unless otherwise agreed by the parties to the contract, the acceptance is deemed:
1- To be given through the Data Message at the time when it enters an Information System outside the control of the originator of the message;
2- To be received by the addressee at the time when the Data Message enters an Information System the parties to the contract agreed to use or enters an addressee’s information system.

Article 12

Contracting may take place between Automated Electronic Media including two or more Electronic Information Systems put in place or programmed in advance to carry out such tasks. Contracting shall be valid and enforceable and have legal effects although no natural person interferes, in person or directly, in the contracting process, unless that contradicts with other relevant laws.

Article 13

The present Law does not oblige any person to send, receive or use an Electronic Record or Signature without his consent to that.

Article 14

1– An Electronic Record shall be legally effective and shall have the effect of the written record if it meets the following conditions:
   A- If the information contained in that record can be retained and stored and can therefore be consulted at any time;
   B- The possibility to keep the Electronic Record in the form in which it was
formed, sent or received or in any form that makes it easy to establish the accuracy of the information contained therein at the time when it was formed, sent or received;

C- The information contained in the record indicate the person who establishes or receives the record, as well as the date and the time when it is sent and received;

D- If it meets all the terms and conditions specified by the relevant authorities.

2- The terms and conditions set out in paragraph (1) of this Article shall not apply to the information accompanying the record which are intended to facilitate the message and its receipt.

**Article 15**

If the sender asks the addressee, through the Data Message, to acknowledge receipt of the message or if the sender has agreed with the addressee on that, the addressee’s acknowledgement of receipt by Electronic Means shall be deemed a fulfilment of that request or agreement.

**Article 16**

As between the sender and the addressee, the latter may deem the Data Message to be that of the sender and to act accordingly if:

1 – The addressee uses an Information Processing System the addressee has agreed with the sender to use to verify that the message is that of the sender;

2 - If the Data Message, as received by the addressee, is the result of actions of a person whose relationship with the sender enables him access to a method used by the sender to establish that the message was issued by the latter.
Article 17

The provisions of the previous article shall not apply to the following cases:
1- If the addressee receives a notice from the sender to the effect that the message is not issued by him, the addressee should act accordingly. The sender remains liable for any prior-to-notice results.
2- If the addressee was aware or he was able to learn through agreed-to actions that the message was not issued by the sender.

Article 18

1- The sender shall bear the legal consequences of his failure to communicate the notice to the addressee in accordance with the provisions of Article (17).
2- The sender shall not be liable for the Data Message that reaches the addressee as a result of the Information Processing System designated to receive the message being broken into.

Article 19

Acknowledgement of receipt shall not per se deemed proof that the content of the message received by the addressee is identical to the content of that sent by the sender.

Chapter Three: The Authority

Article 20

Under the provisions of this Law, shall be regulated an authority called “the General Authority of Electronic Certification”. The Authority shall have its own budget as part of the general budget of the Palestinian National Authority and shall
have an independent legal personality and full legal capacity to carry out all actions and activities that fulfil all the duties for which the Authority was established.

**Article 21**

1- The Authority shall charge fees for the services it provides. The fees shall be determined by a regulation issued by the Council of Ministers.

2- The Council of Ministers shall issue regulations that define the mechanisms of the creation of the Authority and the make-up of its board of directors, as well as its functions and powers.

**Chapter Four**

**The Transferable Electronic Instrument**

**Article 22**

1- The Electronic Instrument shall be negotiable if it meets the conditions applicable to the negotiable written instrument in accordance with the provisions of the Commercial Law, with the exception of the writing requirement, provided that the person has agreed to its negotiability.

2- If the data contained in the Electronic Instrument can be retrieved, retaining it in accordance with the provisions of Article (14) of this Law shall be deemed a legal action.

3- The provisions of Articles 23, 24, 25, 26 and 27 shall only apply to the commercial bill with the consent of the Monetary Authority which specifies its foundations under instructions issued for this purpose.
Article 23

Without prejudice to the provisions on transferring the right to written instruments, the instrument holder shall be deemed authorized to use the rights related to the transferrable instrument if the Information Processing System used to establish and transfer the instrument is qualified to establish the transfer of the right to that instrument and verify the identity of the beneficiary or the transforee.

Article 24

1- The Electronic Processing System is deemed qualified to establish the transfer of the right to the instrument pursuant to the provisions of Article 23 of this Law if the said system allows for establishing, saving and transferring the Electronic Instrument, subject to the two following conditions combined:

A- If the reliable copy of the transferrable instrument is specified in an unalterable manner, subject to the provisions of paragraph 3 of this Article.

B- If the reliable copy of the instrument indicates the name of the person for whom the instrument was withdrawn and indicates that the instrument is transferrable and if that copy contains the name of the beneficiary.

2- The reliable copy shall be sent and saved by the person who is entitled to it or by the consignee for the person entitled to the instrument.

3- The copies of the reliable copy subject of modification or addition, with the consent of the person entitled to dispose of the instrument, shall be reliable.

4- Each copy of the instrument shall be labelled as reliable or not reliable.

5- Each copy of the reliable copy shall be labelled as being an exact copy of the reliable one.
Article 25
The Electronic Instrument holder entitled by virtue of a transferrable instrument shall be deemed entitled to all rights and defences enjoyed by the holder of the written instrument, pursuant to any legislation in force if that instrument meets all the relevant conditions, unless the agreement stipulates otherwise.

Article 26
The creditor and the debtor by a transferrable Electronic Instrument shall enjoy the rights and defences enjoyed by the creditor and the debtor by a transferrable written instrument.

Article 27
If somebody objects to the implementation of the transferrable Electronic Instrument, the objector should provide sufficient evidence as to the invalidity of the instrument. The party requesting the implementation of the Electronic Instrument may prove the validity of its instrument by presenting the reliable copy of the transferrable instrument as well as the instrument-related business activity records to ascertain the terms of the instrument and the identity of its holder.

Article 28
Without prejudice to the provisions of this Law, the provisions of the Securities Law shall apply to electronically circulated securities.
Chapter Five: Electronic Money Transfer

Article 29
1- The transfer of money by Electronic Means shall be deemed an acceptable payment means. This Law in no way affects the rights of persons determined under the relevant legislation in force.
2- Electronic payment by any electronic payment means shall be deemed valid and shall have legal effects.
3- The electronic payment means are as follows:
   A- Electronic cheque;
   B- Electronic payment card; and
   C- Other means of payment determined by the Monetary Authority.

Article 30
Each financial institution conducting electronic money transfer business in accordance with the provisions of this Law and the regulations issued pursuant thereto must:
1- Comply with the provisions of the Monetary Authority Law, the Banking Act and relevant laws, regulations and instructions issued based on them.
2- Take measures to provide safe services to customers and maintain banking secrecy.

Article 31
The customer of the financial institution shall not be deemed liable for any illegal record on his account by electronic transfer made after the customer has notified the financial institution of the possibility of others breaking into his account, of
having lost his card, or of the eventuality of others knowing his card’s ID code and has asked the institution to stop using the electronic transfer means.

**Article 32**
Notwithstanding the provisions of Article 31 of this Law, the customer of the financial institution shall be liable for any illegal use of his account by electronic transfer if it is proved that his neglect has substantially contributed to that and that the institution has fulfilled its duties to prevent any illegal use of that account.

**Article 33**
The Monetary Authority shall issue instructions necessary to regulate the electronic money transfer business, including the adoption of electronic payment means, error-correcting and information-disclosure procedures, and any other electronic banking business-related matters including information which financial institutions are obliged to provide.

**Chapter Six**
Electronic Signature

**Article 34**
The signatory must, when using his Signature Creation Device, take into account the following points in order to create a signature with a legal effect:
1- Keep the Signature Creation Device to avoid unauthorized use of it;
2- Notify the persons and authorities concerned without undue delay if:
    A- the Signatory becomes aware that his Signature Creation Device has been
breached;
B- the circumstances and evidence known to the Signatory suggest that his Signature Creation Device has been breached.

3- Where a certificate is used to support a Signature Creation Device, take all measures necessary to ensure the accuracy and completeness of all substantial data and statements made by the Signatory which are relevant to the certificate throughout its life cycle;
4- The signatory shall bear the legal consequences of his failure to satisfy the requirements of this article.

Article 35
For the Electronic Signature to be reliable, the terms and norms determined by the Authority must be satisfied.

Article 36
The Electronic Signature shall be deemed as legally reliable as the written one in the following cases:
1- Where a Signature Creation Device is exclusively used by the signatory;
2- Where the signatory has exclusive control of the Signature Creation Device;
3- There exists a technical possibility to find out or establish any alteration or modification to the signed message and the Electronic Signature related thereto taking place after the time of signing.
Article 37
Where an Electronic Signature is supported by a certificate, the relying party in respect of such signature shall bear the legal consequences of its failure to take steps necessary to verify the validity and enforceability of the certificate, as to whether it is suspended or revoked, and of observing any limitations with respect to the certificate.

Chapter Seven
Electronic Transactions Protection Means

Article 38
The following ways must be used to protect information systems:
1- Encryption by means of public key;
2- Firewalls;
3- Information filters;
4- Denial prevention means;
5- Back-up copies protection measures;
6- Anti-virus software; and
7- Any other means sanctioned by the Authority.

Article 39
Except for encryption keys relating to national security, the officer designated by the relevant authority upon a court order may request the holder of any encryption key to enable him to examine the necessary information related to that key. The possessor must submit the key to the officer.
Article 40
The Electronic Record shall be deemed protected as of the date when it is verified if specific verification procedures agreed to by the parties are applied to ascertain that it was not altered since a specific time.

Chapter Eight
Effect of Foreign Electronic Signatures

Article 41
Without prejudice to the provisions of international agreements in force in Palestine and the principle of reciprocity, licenses issued to licensees by foreign bodies shall be recognized as legally equivalent to national licenses under the same requirements and regulations and in such a way as to ensure the satisfaction of the assurances determined in accordance with the provisions of this Law and the regulations issued thereunder.

Article 42
No regard shall be had to any Electronic Attestation Certificate issued by foreign certification bodies unless the issuer is authorized by the licensing authority in accordance with the terms and conditions defined by the law and the regulations issued thereunder.

Article 43
Without prejudice to relevant laws, no regard shall be had to the place where the Electronic Signature was issued, nor to the jurisdiction in which the issuer of the
Electronic Signature had its place of business.

**Article 44**
In determining whether an Electronic Signature is legally effective, regard shall be had to any agreement between the parties in relation to the transaction in which that Signature was used.

**Article 45**
Signatures complying with the requirements of laws of another state may be recognized as legally equivalent to signatures issued under this Law if the laws of the other state require a level of reliability at least equivalent to that required for such signatures under this Law.

**Article 46**
Notwithstanding the provisions of article 45:

1- Parties to commercial and other transactions may specify that a particular Certification Service Provider, class of Certification Service Providers or class of certificates must be used in connection with Data Messages or signatures submitted to them;

2- The parties may agree to the use of certain types of Electronic Signatures. That agreement shall be recognized as sufficient for the purpose of cross-border recognition between the various jurisdictions, provided that it does not contradict with the applicable laws in Palestine.
Chapter Nine
Government Use of Electronic Records and Signatures

Article 47
The Government may, using electronic records and signatures:
1- Accept the filing, submission, creation or retention of documents;
2- Issue any permit, license, decision or certificate, create or retain documents;
3- Accept fees and any payments;
4- Put out bids and receive tenders relating to Government procurement.

Article 48
In any case where the Government decides to electronically perform any of the functions set out in article 47, the Government may specify:
1- The manner in which records shall be created, filed, retained, submitted or issued;
2- The process by which Government bids are put out, tenders are received, and Government procurement is made;
3- The type of Electronic Signature required, including the requirement that the sender use an electronic signature;
4- The manner in which the Electronic Signature shall be affixed to the record, and the criterion that shall be met by the Electronic Certification Service Provider to whom the document is submitted for filing and retention;
5- Control processes and procedures as appropriate to ensure integrity, safety, security and confidentiality of Electronic Records, payments or fees; and
6. Any other required attributes, conditions or rules for Electronic Records of
payments and fees that are specified for corresponding paper documents.

Chapter Ten
Crimes and Penalties

Article 49
1. Shall be punished by temporary imprisonment:
   A- Whoever commits forgery of or tampers with an Electronic Signature or an Electronic Creation Device or System of the Government or authorities or public establishments, whether by faking, destroying, disfiguring, modifying or altering it or by any other way that leads to altering its data.
   B- Whoever creates or colludes in creating Signature Data or an Electronic Signature System Device of the Government or authorities or public establishments, which he is not entitled to obtain, using false or incorrect information or data.
2- Without prejudice to the provisions of paragraph (1), the punishment shall be imprisonment and fine or either of these two penalties if the Electronic Signatures forged are other than those of the Government or authorities or public establishments.
3- Shall be punished by the penalty decided for the crime of forgery, as the case may be, whoever uses this forged document with his knowledge that the document is forged.

Article 50
Whoever gains access, pursuant to powers conferred under this Law, to
information in Electronic Records, Documents or Communications and deliberately discloses any of those information, shall be punished by imprisonment and a maximum fine of five thousand Jordanian dinars or either of these two penalties.

**Article 51**

Whoever illegally uses somebody else’s personal encryption elements relating to signature shall be punished by imprisonment and a fine not less than three thousand dinars, or either of these two penalties.

**Article 52**

Shall be punished by imprisonment and a maximum fine of five thousand dinars or either of these two penalties whoever:

1- unlawfully discloses decryption keys or decrypts information filed with him;
2- unlawfully uses personal encryption elements related to somebody else’s signature;
3- deliberately decrypts encrypted data in any way other than the cases authorized by law;
4- unlawfully uses a Signature Creation Device pertaining to the signature of another person.

**Article 53**

Shall be punished by imprisonment and a maximum fine of three thousand dinars or either of these two penalties whoever deliberately establishes or publishes a certificate or commits forgery by incorrect electronic information for an unlawful purpose.
Article 54
The penalty shall be imprisonment for one year at most and a maximum fine of one thousand Jordanian dinars or its equivalent in the legally circulated currency or either of these two penalties in case of failure to notify the Authority of any change in the data the person obtained based on a license to provide services relating to electronic transactions to the public.

Article 55
Shall be punished by imprisonment and a maximum fine of five thousand Jordanian dinars or its equivalent in the circulated currency or either of these two penalties whoever manages, using the computer network or an information technology means, to take over, either for himself or for others, an Electronic Signature, Electronic Signature Creation Data, an Electronic Signature Creation System or an Electronic Document or to break into, intercept or disable any of them by using fraud, an assumed name or false identity where this would deceive the victim.

Article 56
Without prejudice to the right of bona fide third party, shall be ordered, in all instances, the confiscation of devices, software or means used in the commission of any of the crimes specified in this Law or the money accrued therefrom, as well as the closure of the domain or site in which any of these crimes is committed whether permanent closure or for a specified period as determined by court, if the crime was committed with the knowledge of the owner.
Article 57
The penalty shall be imprisonment for a maximum six months and a maximum fine of one thousand Jordanian dinars for anyone who deliberately provides incorrect information on his identity to an Electronic Certification Service Provider when requesting a certificate or requesting the revocation or suspension of the certificate.

Article 58
Shall be punished by imprisonment and a maximum fine of three thousand Jordanian dinars whoever issues certificates or provides any services related to electronic signatures without authorization from the Authority.

Article 59
Without prejudice to any severer penalty provided for by any other law, whoever commits an act criminalized under the laws in force, using an electronic means, shall be sentenced to a maximum one year in prison and a maximum fine of three thousand Jordanian dinars or its equivalent in the legally circulated currency or by either of these two penalties. He shall be punished by the severer penalty where the penalties prescribed under those laws are higher than that provided for under this Article.

Article 60
The authority may, without need for a court warrant, shut down any shop or company that provides Electronic Certification services without a license.
Article 61
The Authority may, if the licensee violates the terms of the license or the provisions of this Law, revoke the license or suspend it until the situation involving the violation is rectified, in accordance with the provisions prescribed by the Regulations of this Law.

Article 62
Without prejudice to any severer penalty provided for by any other law, shall be sentenced to three years in prison at most and a maximum fine of three thousand dinars or either of these two penalties whoever deliberately prevents a judicial officer or persons authorized to provide assistance from conducting inspections.

Article 63
For the application of the provisions of this Law, the Authority may grant a number of its officials the capacity of judicial officers. Civil authorities and security services are required to provide them with all possible assistance to perform their duties.

Article 64
The Council of Ministers shall issue the regulations necessary to enforce this Law.

Article 65
All provisions contravening the provisions of this Law are hereby abrogated.
Article 66

All relevant authorities, each in its respective field of competence, are required to implement this Law, which shall be published in the Official Gazette and take effect from the date of publication.

Issued in Ramallah on / /2010 AD
Corresponding to / /1431 AH

Mahmud Abbas  
President of the State of Palestine  
Chairman of the Executive Committee of the Palestine Liberation Organisation  
President of the Palestinian National Authority