Electronic Transactions and Electronic Signatures Act

Act No. [ ] of [ ]

An Act to provide for the facilitation of the use of electronic transactions and signatures and for related matters.

ENACTED by [ ]

CHAPTER 1: GENERAL PROVISIONS

Article 1: The Basis

This Act is enacted pursuant to [please state relevant articles of constitution].

Article 2: Purpose

The purpose of this Act is to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to:

(a) Recognize the importance of the information economy and information society for the economic and social prosperity of Afghanistan;

(b) Develop a safe, secure and effective environment for electronic transactions.

(c) Promote the understanding, acceptance of and growth in the number of electronic transactions in Afghanistan;

(d) Remove and prevent barriers to the use of electronic communications in Afghanistan resulting from uncertainties over writing and signature requirements;

(e) Promote legal certainty and confidence in the integrity and reliability of data messages and electronic commerce, and foster the development of electronic commerce through the use of electronic signatures;

(f) Promote technology neutrality in the application of legislation to electronic communications and transactions;

(g) Promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

(h) Ensure that electronic transactions in Afghanistan conform to the highest international standards; and

General comment: this Act is in line with applicable policies and strategies. In particular, it implements Action Lines 2.1, 2.2 and 2.3 (facilitation of the use of electronic documents and electronic signatures) of the Electronic Government Strategy Draft for Afghanistan (2011).

This Act is based on UNCITRAL texts, namely, the UNCITRAL Model Law on Electronic Commerce, which has already been enacted in more than 60 States, including many in Asia, the UNCITRAL Model Law on Electronic Signatures, and the United Nations Convention on the Use of Electronic Communications in International Contracts (the "Electronic Communications Convention"), also adopted by several Asian States. Additional information on UNCITRAL texts, including each provision referred to as a model of the articles of the Act, is available on the UNCITRAL website at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html.

By adopting an Act based on UNCITRAL texts, Afghanistan will enjoy uniformity of provisions with many other jurisdictions that have enacted the same texts. This will give the possibility to benefit from the experience of those other jurisdictions in the implementation and application of the Act, as evidenced by judicial decisions and academic writings. It will also, among others, facilitate cross-border electronic commerce, which is fundamental to develop the economy of a land-locked country.

Article 3: Preliminary

This Act may be cited as the [Electronic Transactions and Electronic Signatures Act], [2015] and shall come into operation on such a date as [the Minister] may, by notice published in the Gazette, appoint.

Article 4: Definitions

In this Act, unless the context otherwise requires:

- "addressee", in respect of an electronic communication, means a person who is intended by the originator to receive the electronic communication, but not a person acting as an intermediary in respect of that electronic communication;

- "ARCA" means the Afghanistan Root Certification Authority established under the Ministry of Communications and Information Technology;

- "automated message system" means a computer program, an electronic or other automated means used to initiate an action or respond to data messages or performance in whole or in part, without review or intervention by a person each time an action is initiated or a response is generated by the system;
- "certificate" means a data message or other record confirming the link between a signatory and signature creation data;
- "certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

- "consumer" means any natural person who is acting for purposes which are outside his or her trade, business or profession;

- "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable handheld calculator, a device which is non-programmable or which does not contain any data storage facility, or such other device as the Minister may, by notification in the Gazette, prescribe;

- “cryptography provider” means any person, group or institution that provides or proposes to provide cryptography services in Afghanistan;

- “cryptography service” means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring:

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;

(b) that the authenticity or integrity of such data or data message is capable of being ascertained;

such services may include the provision of electronic encryption methods, electronic encryption systems, and secure electronic environments, or services related thereto, but do not include the supply of, or of any right to use, computer software or computer hardware except where the supply is integral to the provision of cryptography services not consisting in such supply;

- “data message” means information generated, sent, received or stored by electronic, magnetic, optical or similar means including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy;

- “domain name” means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

- “e-government services” means any public service provided by electronic means by any public body in Afghanistan;
- "electronic address" means an address, including but not limited to an electronic mail address or a mobile telephone number, to which an electronic communication can be sent;

- “electronic communication” means a communication by means of data messages;
- “electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s intention in respect of the information contained in the data message;

- “information system” means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages;

- “intermediary” means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

- “Minister” means the Minister of Communications and Information Technology;

- “originator” means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

- “person” includes a natural and legal person;

- “public body” means a department or a ministry of the Government, organ of State or statutory corporation;

- "recipient", in relation to an electronic message, means an authorized user of the electronic address to whom the message is sent, and where a recipient of an electronic message has one or more electronic addresses in addition to the address to which the message was sent, the recipient shall be treated as a separate recipient with respect to each such address;
- “relying party” means a person that may act on the basis of a certificate or an electronic signature;

- “rule of law” includes written law;

- “security procedure” means a procedure for the purpose of verifying that a data message is that of a specific person; or detecting error or alteration in the communication, content or storage of a data message since a specific point in time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgment procedures, or similar security devices;

- "sender", in relation to an electronic message, means a person who sends the message, causes the message to be sent, or authorizes the sending of the message;
- “signatory” means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

- “transaction” means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;

- "verify a digital signature", in relation to a given digital signature, record and public key, means to determine accurately that the digital signature was created using the private key corresponding to the public key listed in the digital certificate and that the data message has not been altered since its digital signature was created.

> **Comment**: this article specifies the meaning of terms used throughout the Act. Only terms actually used in the Act are defined. The definitions are meant to apply as well in any subsidiary legislation, and appropriate cross-references should be made in any relevant subsidiary legislation to that end.

Article 5: Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

(3) This Act must not be interpreted so as to exclude any other statutory or judge made law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act, provided that, and only in respect of the subject matters dealt with hereunder, and only in the contexts dealt with hereunder, the provisions of this Act shall prevail over any other previously enacted laws or judge-made law only to the extent of any such inconsistency.

Comment: paragraphs 1 and 2 refer to the fact that the Act is an enactment of UNCITRAL texts. When implementing the UNCITRAL-based provisions of the Act, it is therefore possible, and indeed useful, to compare the interpretation and application of the same provisions in other jurisdictions. This approach allows to build expertise quickly in a new sector while not limiting the independence of the judiciary. Paragraphs 1 and 2 correspond to article 3 of the UNCITRAL Model Law on Electronic Commerce.

Article 6: Exclusions

(1) This Act shall not apply to any of the following matters:

1. Power of attorney
2. Personal status matters
3. Negotiable instruments
4. Sale or other permanent disposition of real estate

(2) The Minister may by order modify the provisions of paragraph (1) by adding to, deleting or amending any class of transactions or matters specified herein.

Comment: the list of matters excluded from the scope of application of the Act currently features topics commonly excluded from the scope of similar laws. The exclusion of personal status matters intends to cover family law, law of inheritance, etc. The exclusion of permanent disposition of real estate allows for concluding electronically contracts of lease of immovable property. The Minister is given the authority to modify the list in order to fine-tune the scope of the Act to actual needs as well as to reflect technological developments. The need to formally amend the Act in Parliament might delay legislative adjustment to those needs and developments.

Article 7 – Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under another law.

Comment: the principle of party autonomy, or freedom of contract, is a general principle that applies to all commercial transactions. It may also apply to electronic transactions with consumers and public bodies unless other law limits it. The principle requires actual agreement of the parties, i.e. all parties must actually consent to the variation.
Article 7 is inspired by article 4 of the UNCITRAL Model Law on Electronic Commerce.

CHAPTER 2: RECOGNITION AND FACILITATION OF ELECTRONIC TRANSACTIONS

General comment: this chapter aims at setting forth the fundamental legal notions necessary to give legal recognition to electronic transactions. In particular, it establishes the three fundamental principles of non-discrimination of electronic communications, of technology neutrality and of functional equivalence that are widely regarded as the pillars of the law of electronic communications.
As the law will apply also to transactions with public bodies (i.e., e-government), reference is often made to the notion of "data message", which is the broadest technology-neutral notion and allows to encompass all types of transactions (commercial, consumers and e-government).

Article 8: Legal Recognition of Data Messages

(1) Information shall not be denied legal effect, validity or enforceability solely on the ground that it is wholly or partly in the form of a data message.

(2) Information shall not be denied legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

Comment: article 8 sets forth the principle of non-discrimination of electronic communications, including linked information. It corresponds to articles 5 and 5 bis of the UNCITRAL Model Law on Electronic Commerce.

Article 9: Writing

Where a rule of law requires information to be in writing or provides for certain consequences if it is not, a data message satisfies that requirement if the information contained therein is accessible via electronic means so as to be usable for subsequent reference.

Comment: article 9 sets forth the requirements to establish functional equivalence between electronic and written form. It corresponds to article 6, paragraph 1 of the UNCITRAL Model Law on Electronic Commerce.

Article 10: Electronic Signatures

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
   (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
   (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
   (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
   (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
4. Paragraph 3 does not limit the ability of any person:
   (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or
   (b) To adduce evidence of the non-reliability of an electronic signature.

Comment: the above article, which is based on article 6 of the UNCITRAL Model Law on Electronic Signatures, introduces a "two tier" approach under which all electronic signatures may have legal recognition in light of circumstances, and those offering a higher level of security are associated with certain legal presumptions with respect to origin and integrity.
Thus, the use of authentication technology based on encryption techniques and Public Key Infrastructure would fall under article 10(3) and benefit from associated presumptions. In this manner, the law remains technology neutral but acknowledges benefits associated with secure technologies.

Commercial and private parties may freely agree on the use of the signature technologies and methods of their choice as provided in article 7 of the Act.
Special requirements might apply to communications exchanges with public bodies if so requested according to article 33 of the Act.

Article 11: Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Comment: article 11, which corresponds to article 8 of the UNCITRAL Model Law on Electronic Commerce, sets forth the requirements for the functional equivalence of the paper-based notion of "original" in an electronic environment.

Article 12: Admissibility and Evidential Weight Accorded to Electronic Communications and Data Messages

(1) Information in the form of an electronic communication or a data message shall be accorded due evidential weight.

(2) Rules or laws of evidence must not be applied so as to deny the admissibility of an electronic communication or a data message in evidence in any legal proceedings on the mere grounds that it is constituted by an electronic record or a data message, or, if it is the best

evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(3) In assessing the evidential weight of an electronic communication or a data message, regard must be had to:

(a) the reliability of the manner in which the electronic communication or data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the electronic record or data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

Comment: article 12 is inspired by article 9 of the UNCITRAL Model Law on Electronic Commerce. In practice, it should be noted that usually electronic evidence is not evaluated in itself, but rather in the context of additional evidence (written documents, oral testimony, etc.).

Article 13: Retention of Data Messages

(1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of data messages if the following conditions are satisfied:

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the data message is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and

(c) such information, if any, as enables the identification of the origin and destination of a data message and the date and time when it was sent or received, is retained.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) (c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, if the conditions in subparagraphs (a) to (d) of that paragraph are complied with.

(4) Nothing in this article shall:

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of data messages; or

(b) Preclude any public body from specifying additional requirements for the retention of data messages that are subject to the jurisdiction of such public body.

Comment: article 13 corresponds to article 10 of the UNCITRAL Model Law on Electronic Commerce. Paragraph 4 provides a safety clause for archival of documents from public bodies and for the archival of the electronic equivalents of paper-based documents with special retention requirements.

CHAPTER 3: COMMUNICATIONS AND CONSEQUENCES OF DATA MESSAGES

General comment: this chapter aims at clarifying the mechanism for the formation and validity of contracts concluded with the use, in part or exclusively, of electronic means. The relevant provisions are inspired by the UNCITRAL Model Law on Electronic Commerce, as updated and complemented by the UN Convention on the Use of Electronic Communications in International Contracts (the "Electronic Communications Convention"). Those rules, which have been adopted in a large number of jurisdictions, do not affect general contract law, but complement it.

Article 14: Formation and Validity of Contracts

(1) In the context of the formation of contracts, an offer and the acceptance of an offer may be expressed by means of a data message.

(2) Nothing in this law requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.

Comment: Article 14(1) contains an application of the general rule contained in article 8 of the Act. Article 14(2), based on article 8(2) of the Electronic Communications Convention, specifies that the use of electronic means is voluntary, but does not have to be explicit. For instance, sending or replying to an electronic mail may be interpreted, in light of all circumstances, as implied consent to using that electronic mean.

Article 15: Location of Party Using Electronic Communications

(1) For the purposes of locating the place of business of a party using electronic communications, a location is not a place of business merely because that is where equipment and technology supporting an information system used by a party in connection with the

formation of a contract are located, or where the information system may be accessed by other parties.

(2) For the same purposes, the sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Comment: article 13 contains rules on party location when using electronic communications. It repeats article 6 of the Electronic Communications Convention.

Article 16: Attribution

(1) A data message is that of the originator if it was sent by the originator himself.
(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent -

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator and to act on that assumption if -

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) shall not apply -

(a) from the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly;

(b) in a case within subparagraph (3)(b), at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator; or

(c) if, in all the circumstances of the case, it is unconscionable for the addressee to regard the data message as being that of the originator or to act on that assumption.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that the addressee duplicates another data message and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Comment: article 16 corresponds to article 13 of the UNCITRAL Model Law on Electronic Commerce.

Article 17: Acknowledgement of Receipt

(1) Subparagraphs (2), (3) and (4) shall apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by any communication by the addressee, automated or otherwise; or any conduct of the addressee, when that communication or conduct is sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgment, the data message is treated as though it had never been sent, until the acknowledgment is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and

(b) if the acknowledgment is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it has never been sent or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgment of receipt, it is presumed, unless evidence to the contrary is adduced, that the related data message was received by the addressee, but that presumption does not imply that the content of the data message corresponds to the content of the record received.

(6) Where the received acknowledgment states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed, unless evidence to the contrary is adduced, that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgment of its receipt.

Comment: article 17 corresponds to article 14 of the UNCITRAL Model Law on Electronic Commerce.

Article 18: Time and place of dispatch and receipt

1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.

4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication

Comment: article 18 reflects article 10 of the Electronic Communications Convention, which is the most recent UNCITRAL provision dealing with the determination of the time and place of dispatch and receipt of an electronic communication.

Article 19: Invitations to Make Offer

A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

Comment: article 19 corresponds to article 11 of the Electronic Communications Convention.

Article 20: Automated Transactions

A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed each of the individual actions carried out by the automated message systems or the resulting contract.

Comment: article 20 corresponds to article 12 of the Electronic Communications Convention.

Article 21: Errors in Electronic Communications

(1) Where a natural person makes an input error in electronic communications exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the data message in which the input error was made if:

(a) the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the data message;

(b) the person, or the party on whose behalf that person was acting, takes reasonable steps, including steps that conform to the other party's instructions, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services; and

(c) the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.

(2) Nothing in this article affects the application of any rule of law that may govern the consequences of any errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in paragraph 1.

Comment: article 21 corresponds to article 14 of the Electronic Communications Convention.

Article 22: Availability of Contract Terms

Nothing in this Act affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of data messages to make available to the other contracting party those data messages that contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

Comment: article 22 corresponds to article 13 of the Electronic Communications Convention.

CHAPTER 4: ELECTRONIC SIGNATURES

General comment: the Act adopts a technology neutral approach, closely inspired by the UNCITRAL Model Law on Electronic Signatures. These provisions are meant primarily for commercial exchanges and exchanges with other private parties; exchanges with public bodies may be subject to special authentication requirements.

Article 23 – Scope of application of electronic signatures

This chapter applies where electronic signatures are used in the context of commercial and non-commercial activities. It does not override any rule of law intended for the protection of consumers.

Comment: article 23 corresponds to article 1 of the UNCITRAL Model Law on Electronic Signatures. For the applicability of this article to public bodies, see article 33 (1)(b) giving the authority to establish special rules for electronic signatures. In absence of those rules, article 23 will apply, subject, of course, to the general declaration of readiness of a public body to accept electronic communications set forth in article 33.

Article 24 – Equal treatment of signature technologies

Nothing in this law shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 10 or otherwise meets the requirements of applicable law.

Comment: article 24 corresponds to article 3 of the UNCITRAL Model Law on Electronic Signatures. It implements the principle of non-discrimination in the field of electronic signatures.

Article 25 – Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;
(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 26, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
(i) The signatory knows that the signature creation data have been compromised; or
(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.
2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Comment: article 25 corresponds to article 8 of the UNCITRAL Model Law on Electronic Signatures.

Article 26 – Conduct of the certification service provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:
(a) Act in accordance with representations made by it with respect to its policies and practices;
(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;
(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:

(i) The identity of the certification service provider;

(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;

(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) The method used to identify the signatory;

(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) That the signature creation data are valid and have not been compromised;

(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) Whether means exist for the signatory to give notice pursuant to article 25, paragraph 1 (b), of this Act;

(vi) Whether a timely revocation service is offered;

(e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 25, paragraph 1 (b), of this law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

(f) Utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Comment: article 26 and the closely-related article 27 set forth basic standards for third party service providers, including third parties issuing PKI-based certificates. Technical details may be specified in secondary level legislation (regulations) issued by the competent authority (i.e., the Minister or ARCA).

Article 26 corresponds to article 9 of the UNCITRAL Model Law on Electronic Signatures.

Article 27 – Trustworthiness

For the purposes of article 26, paragraph 1 (f), of this Act, in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(a) Financial and human resources, including existence of assets;

(b) Quality of hardware and software systems;

(c) Procedures for processing of certificates and applications for certificates and retention of records;

(d) Availability of information to signatories identified in certificates and to potential relying parties;

(e) Regularity and extent of audit by an independent body;
(f) The existence of a declaration by ARCA or by the certification service provider regarding compliance with or existence of the foregoing; or
(g) Any other relevant factor.

Comment: article 27 corresponds to article 10 of the UNCITRAL Model Law on Electronic Signatures. Article 27 may also provide guidance to ARCA in discharging its oversight functions.

Article 28 – Conduct of the relying party

A relying party shall bear the legal consequences of its failure:
(a) To take reasonable steps to verify the reliability of an electronic signature; or
(b) Where an electronic signature is supported by a certificate, to take reasonable steps:
(i) To verify the validity, suspension or revocation of the certificate; and
(ii) To observe any limitation with respect to the certificate.

Comment: article 28 corresponds to article 11 of the UNCITRAL Model Law on Electronic Signatures.

Article 29 – Recognition of foreign electronic signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
(a) To the geographic location where the certificate is issued or the electronic signature created or used; or
(b) To the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside Afghanistan shall have the same legal effect in Afghanistan as a certificate issued in Afghanistan if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside Afghanistan shall have the same legal effect in Afghanistan as an electronic signature created or used in Afghanistan if it offers a substantially equivalent level of reliability.
4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.
5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.
6. Paragraphs 1 to 5 of this article do not apply to electronic communications exchanged with Afghan public bodies.

7. The Minister may, by regulations, provide that the Afghanistan Root Certification Authority (ARCA) may recognise certification authorities outside Afghanistan that satisfy the prescribed requirements for any of the following purposes:

(a) the recommended reliance limit, if any, specified in or in respect of a digital certificate issued by the certification authority, or any encryption methods or systems or any means or technology for building or deploying a secure electronic environment provided by the certification authority;

(b) the presumptions referred to in article 10(3).

Comment: this provision is made of two parts. Both parts are meant to be technology and location neutral.
The first part, comprising paragraphs 1 to 5, applies only to transactions concerning private and commercial parties and corresponds to article 12 of the UNCITRAL Model Law on Electronic Signatures. Private parties may agree on which technology or authentication method they may use for cross-border transactions.
The second part, comprising paragraphs 6 and 7, creates a mechanism for the recognition of foreign electronic signatures exchanged with Afghan public entities. It also allows to attribute the presumptions established in article 10(3) without having to verify the actual level of reliability of the electronic signatures.

Article 30 – Supervisory Authority

(1) ARCA shall be the supervisory authority for the purposes of this law and, in particular, for the purposes of licensing, certifying, monitoring and overseeing the activities of certification authorities.
(2) A certification service provider having its main place of business in Afghanistan shall register itself with the supervisory authority within [specify period] of commencing operations in Afghanistan and shall be subject, in addition to any obligations under this Act, to any orders or directions issued by the Ministry from time to time, provided that in the event of any inconsistency between any such directive or order and this Act, this Act shall prevail to the extent of any such inconsistency.

Comment: the first paragraph of article 30 is the founding provision for setting up a supervisory authority in charge, in particular, of overseeing certification service providers. This has been identified in ARCA. The second paragraph of article 30 gives legal basis to the oversight of the competent agency (to be identified and designated) over certification service providers. It also gives that agency statutory authority to adopt secondary level legislation of technical content.

Article 31 – Existing Certification Authorities

Certification authorities that are providing cryptography services in Afghanistan are deemed to be cryptography providers under this Act and need not re-register or seek additional licenses in respect of their cryptography services provision provided their cryptography services provision is covered and authorised under their license and registration as certification authorities. For

the avoidance of doubt, cryptography providers are not deemed to be certification authorities unless they are registered and licensed as certification authorities

CHAPTER 5: E-GOVERNMENT SERVICES

General comment: this chapter ensures that the general principles of electronic transactions are applicable also to the public sector. This is particularly important in certain B2G applications critical for trade such as single windows for customs operations.

By adopting this chapter, the following actions lines of the strategy for e-government in Afghanistan will be implemented:

Action Line 2.1: Digital Signature Act – gives electronic signatures the same legal status as written signatures and sets a uniform legal standard for electronic signatures and records;

Action Line 2.2: Electronic Transaction Act – facilitates electronic communications by means of reliable electronic records and promotes public confidence in the integrity and reliability of electronic records, ecommerce and e-Government;

Action Line 2.3: Electronic Documents Act – facilitates the use of electronic documents. (See e-Government Strategy Draft for Afghanistan, at page 44, under section 3.5.2 – "Enabling Environment").

While the general principles of the Act will apply also to e-procurement, the Act does not contain any specific provision on e-procurement. Hence, specific provisions for e-procurement may be prepared and implemented by the relevant authority, and shall be cross-referenced to this Act as appropriate.

Article 32: Acceptance of Filing and Issuing of Documents

(1) Any public body that, pursuant to any law:

(a) accepts the filing of documents, or requires that documents be created or retained, or is responsible for administration and management of documents;

(b) issues any permit, licence or approval; or

(c) provides for a manner of payment,

may, notwithstanding anything to the contrary in such law:

(i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;

(ii) manage and administer such documents in the form of data messages;

(iii) issue such permit, licence or approval in the form of a data message; or

(iv) make or receive payment in electronic form or by electronic means.

Article 33: Requirements may be specified

(1) In any case where a public body performs any of the functions referred to in article 32, such body may specify by [notice in the Gazette] the requirements that documents filed with the public body in the form of data messages must conform to, including without limitation the following-

(a) the manner and format in which the electronic communications must be filed, administered, managed, created, retained or issued;

(b) in cases where the data messages has to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(c) the manner and format in which electronic signatures referred to in subparagraph (b) must be attached to, incorporated in or otherwise associated with the data message;

(d) the identity of or criteria that must be met by any certification service provider used by the person filing the document, or that such certification service provider must be a preferred certification service provider designated in accordance with subparagraph (2);

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for documents, data messages or payments.

(2) For the purposes of subparagraph (1)(d) the Minister may designate a certification service provider as a preferred certification service provider.

(3) Nothing in this Act shall by itself compel any public body to accept, administer, manage or issue any document in the form or data messages.

> **Comment:** article 33 specifies that public bodies are not compelled to use electronic communications because of this Act. A dedicated notice is required to inform of their readiness to do so.
> Although public bodies may specify the timing and modalities of their readiness to provide e-government services, it is recommended that commonality of fundamental principles for all types of electronic transactions shall be preserved. This may require cross-referencing to this Act in the legislation enabling e-government services.