THE ELECTRONIC TRANSACTIONS ORDINANCE, 2002

THE ELECTRONIC TRANSACTIONS ORDINANCE, 2002

(ORDINANCE NO.LI)

CHAPTER I
PRELIMINARY

1. Short title, extent and commencement:—(1) This Ordinance may be called the Electronic Transactions Ordinance, 2002.

(2) It extends to the whole of Pakistan.

(3) It shall come into force at once.

2. Definitions:—(1) In this Ordinance, unless there is anything repugnant in the subject or context,—

(a) "Accreditation certificate" means a certificate granted by the Certification Council to a Certification Service Provider;

(b) "accredited Certification Service Provider" means a Certification Service Provider accredited under this Ordinance to issue certificates for the use of its cryptography services;

(c) "addressee" means the person intended by the originator to receive the electronic communication but does not include an intermediary;

(d) "advanced electronic signature" means an electronic signature which is either—

(i) unique to the person signing it, capable of identifying such person, created in manner or using a means under the sole control of the person using it, and attached to the electronic document to which it relates in a manner that any subsequent change in the electronic document is detectable ; or

(ii) provided by an accredited certification service provider and accredited by the Certification Council as being capable of establishing authenticity and integrity of an electronic document;

(e) "appropriate authority" means—

(i) in relation to items contained in the Federal Legislative List of the Constitution of the Islamic Republic of Pakistan, 1973, the Federal Legislature or Federal Government;

(ii) is relation to items contained in the Concurrent Legislative List of the Constitution of the Islamic Republic of Pakistan, 1973, for which a Federal law is in force, the Federal Legislative or Federal Government, and, in all other cases, respective Provincial Legislature or Provincial Government;

(iii) in relation to the functions of the Federal Government or respective Provincial Governments being discharged by a statutory body that statutory body; and

(iv) in relation to matters in respect whereof the Supreme Court or the High Courts are empowered to make rules for regulation of their proceedings, the Supreme Court or High Court, as the case may be;

(f) "authenticity" means, in relation to an electronic document or electronic signature, the identification of and attribution to a particular person or information system;

(g) "automated" means without active human intervention:

(h) "certificate" means a certificate issued by a Certification Service Provider for the purpose of confirming the authenticity or integrity or both, of the information contained therein, of an electronic document or of an electronic signature in respect of which it is issued;

(i) "Certification Council" means the Electronic Certification Accreditation Council established under Section 18;

(j) "certification practice statement", means the statement prepared by a certification service provider specifying the practices it employs in relation to the issuance of certificates and matters connected therewith;

(k) "cryptography services" means services in relation to the transformation of contents of an electronic document from its original form to one that cannot be understood or decoded by any unauthorized person;

(l) "electronic" includes electrical, digital, magnetic, optical, biometric, electro-chemical, wireless or electromagnetic technology;

(m) "electronic document" includes documents, records information communications or transactions in electronic form;

(n) "electronic signature" means any letters, numbers, symbols, images, characters or any combination thereof in electronic form, applied to, incorporated in or associated with an electronic document, with the intention of authenticating or approving the same, in order to establish authenticity or integrity, or both;

(o) "information" includes text, message, data, voice, sound, database, video Signals, software, computer programs, codes including object code and source code;

(p) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information;

(q) "integrity" mean, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

(r) "intermediary" means a person acting as a service provider in relation to the sending receiving, storing or processing of the electronic communication or the provision of other services in relation to it;

(s) "network service provider" means a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services;

(t) "originator" means a person by whom, or on whose behalf, electronic document purports to have been generated or tent prior to receipt or storage, if any but does not include an intermediary;

(u) "person" includes an individual, appropriate authority, trust, waqf, association. statutory body, firm, company including joint venture or consortium or any other entity whether registered or not:

(v) "prescribed" means prescribed by rules made under this Ordinance;

(w) "repository" means an information system for storing and retrieving certificates or other information related, thereto established under section 23;

(x) "security procedure" means a procedure which:

(i) is agreed between parties;

(ii) is implemented in the normal course by a business and which is reasonably secure and reliable; or

(iii) in relation to a certificate issued by a certification service provider is specified in its certification practice statement:

for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or, codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software hardware or similar security devices;

(y) subscriber's means a person, who subscribes to the services of a certification service provider;

(z) "transaction" means an act or series of acts in relation to creation or performance of rights and obligations; and

(aa) "valid accreditation certificate" means an accreditation certificate which has not been suspended or revoked.

CHAPTER 2
RECOGNITION AND PRESUMPTION

3. Legal recognition of electronic forms.—No document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness.

4. Requirement for writing:—The requirement under any law for any document, record, information, communication or transaction to be in written form shall be deemed satisfied where the document, record, information communication or transaction is in electronic form, if the same is accessible so as to be usable for subsequent reference.

5. Requirement for original form:—(1) The requirement under any law for any document, record, information, communication or transaction to be presented or retained in its original form shall be deemed satisfied by presenting or retaining the same if:

(a) there exists a reliable assurance as to the integrity thereof from the time when it was first generated in its final form ; and

(b) it is required that the presentation, thereof is capable of being displayed in a legible form.

(2) For the purposes of clause (a) of sub-section (1):

(a) the criterion for assessing the integrity of the document, record, information, communication or transaction is whether the same has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display, and

(b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information, communication or transaction was generated and all other relevant circumstances.

6. Requirement for retention:— The requirement under any law that certain document, record, information, communication or transaction be retained shall be deemed satisfied by retaining it in electronic form if;

(a) the contents of the document, record, information, communication or transaction remain accessible so as to be usable for subsequent reference;

(b) the contents and form of the document, record, information, communication or transaction are as originally generated, sent or received, or can be demonstrated to represent accurately the contents and form in which it was originally generated, sent or received; and

(c) such document, record, information, communication or transaction, if any, as enables the identification of the origin and destination of document, record, information, communication or transaction and the date and time when it was generated, sent or received, is retained.

7. Legal recognition of electronic signatures:—The requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signature are applied.

8. Proof of electronic signature:—An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both.

9. Presumption relating to advanced electronic signature:—In any proceedings, involving an advanced electronic signature, it shall be presumed unless evidence to contrary is adduced, that:

(a) the electronic document affixed with an advanced electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; or

(b) the advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time.

10. Stamp Duty:—Notwithstanding anything contained in the Stamp Act, 1899 (II of 1899), for a period of two years from the date of commencement of this Ordinance or till the time the Provincial Governments devise and implement appropriate measures for payment and recovery of stamp duty through electronic means, whichever is later, stamp duty shall not be payable in respect of any instrument executed in electronic form.

11. Attestation and notarization:—Notwithstanding anything contained in any law for the time being in force, no electronic document shall require attestation and notarization for a period of two years from the date of commencement of this Ordinance or till the time the appropriate authority devise and implement measures for attestation and notarization of electronic documents, whichever is later.

12. Certified copies:—Where any law requires or permits the production of certified copies of any records, such requirement or permission shall extend to printouts or other forms of display of electronic documents where, in addition to fulfillment of the requirements as may be specified in such law relating to certification, it is verified in the manner laid down by the appropriate authority.

CHAPTER 3
ELECTRONIC DOCUMENTS

13. Attribution of communications:—(1) Unless otherwise agreed as between an originator and the addressee, an electronic communication shall be deemed to be that of the originator if it was sent:

(a) by the originator himself:

(b) by a person who had the authority to act for and on behalf of the originator in respect of that electronic communication : or

(c) by an automated information system programmed by, or on behalf of the originator.

(2) Unless otherwise agreed as between the originator and the addressee, addressee is to regard an electronic communication as being that of the originator, is entitled to act on that assumption if:

(a) the addressee has no reason to suspect the authenticity of the electronic communication; or

(b) there do not exist any circumstances where the addressee knows, or ought to have known by exercising reasonable care: that the electronic communication was not authentic.

14. Acknowledgment of receipt:—(1) Unless otherwise agreed where the originator has stated that the electronic communication is conditional on receipt of acknowledgment, the electronic communication is treated as though it has never been sent, until the acknowledgment is received.

(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—

(a) any communication automated or otherwise, by the addressee; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic communication is received.

15. Time and place of dispatch and receipt of electronic communication:—(1) Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic communication occurs when it enters an information system outside the control of the originator.

(2) Unless otherwise agreed between the originator and the addressee, or unless proved otherwise, the time of receipt of an electronic communication is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving the electronic communication, receipt occurs;

(i) at the time when the electronic communication enters the designated information system; or

(ii) if the electronic communication is sent to an information system of the addressee that is not the designated information system at the time when the electronic communication is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the electronic communication enters and information system of the addressee.

(3) Sub-section (2) applies notwithstanding that the place where the information system is located may be different from the place where the electronic communication is deemed to be received under sub-section (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic communication is deemed to be dispatched at the place where originator ordinarily resides or has his place of business, and is deemed to be received at the place where the addressee ordinarily resides or has his place of business.

(5) For the purpose of this section:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business reference is to be made to the usual place of residence ; and

(c) "usual place of residence" in relation to a body corporate means the place where it is incorporated or otherwise legally constituted.

16. Electronic documentation of appropriate authority:—(1) Nothing contained Hereinbefore shall confer a right upon any person that any appropriate authority should accept, issue, create, retain, preserve any document in electronic form or effect monetary transaction in electronic form.

(2) Any appropriate authority pursuant to any law or procedure—

(a) accepts the filing of document, or requires that documents be created or retained;

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

(c) provides for the method and manner of payment procurement or transaction may notwithstanding anything contained to the contrary in such law or procedure:

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

(ii) issue such permits, certificate, licence or approval in the form of electronic document: or

(iii) make such payment, procurement or transaction in electronic form.

(3) In any case where an appropriate authority decides to perform any of the functions in clause (i), (ii) and (iii) of sub-section (2) may specify:

(a) the manner and format in which such electronic documents shall be filed created, retained or issued:

(b) when such electronic document has to be signed, the type of electronic signature advanced electronic signature or a security procedure required;

(c) the manner and format in which such signature shall be affixed to the electronic document, and the identity of or criteria that shall be met by any certification service provider used by the person filing the document;

(d) control process and procedures as appropriate to ensure adequate integrity. security an confidentiality of electronic documents procurement, transactions or payments: and

(e) any other required attributes for electronic documents or payments that are currently specified for corresponding paper documents.

CHAPTER 4
CERTIFICATION SERVICE PROVIDERS

17. Certification Service Providers.—(1) Nothing in this Ordinance shall impede or in any way restrict the rights of any certificate service provider to engage in the business of providing certification services without being accredited.

(2) No person shall hold himself out as an accredited certification service provider unless he holds a valid accreditation certificate issued under section 24 by the Certification Council.

CHAPTER 5
CERTIFICATION COUNCIL

18. Establishment of the Certification Council:—(1) Within sixty days of the promulgation of this Ordinance, the Federal Government shall by notification in the official Gazette, constitute an Certification Council to be known as Electronic Certification Accreditation Council.

(2) The Certification Council shall be a body corporate with perpetual succession and a common seal, and shall by the said name sue or be sued.

(3) The Certification Council shall comprise of five members with four members form the private sector. One of the Members shall be designated as the chairman.

(4) The members of the Certification Council shall be appointed by the Federal Government for a term of three years and shall be eligible for reappointment once for another term of three years after the expiry of their first term of appointment.

(5) No act or proceeding of the Certification Council shall be invalid by reason only of the existence of any vacancy among its members or any defect in its constitution discovered after such act or proceeding of the Certification Council.

(6) Except for the grant renewal, revocation or suspension of accreditation the Certification Council may from time to time delegate one or more of its functions and powers to one or more of its members.

(7) A member of the Certification Council shall not be removed except on the grounds of misconduct.

(8) No member once appointed shall have any direct financial interest in any concern or business relating to cryptography services.

(9) Decisions of the Certification Council shall be taken by a majority of the members however in case of tie the Chairman shall have a casting vote.

(10) Save as provided herein, the terms and conditions of service of the members of the Certification Council shall be such as may be prescribed.

19. Qualifications of member:— of the five members of the Certification Council:

(a) one shall he telecommunications engineer with at least seven years work experience of which at least one year is in the field of cryptography services;

(b) two shall be professional or academics with at least seven years work experience in the field of information technology;

(c) one shall have an administrative background with at least seven years experience in a private or public organization : and

(d) one member shall be an advocate with at least seven years experience and adequate knowledge of laws relating to information technology and telecommunications.

20. Funds of the Certification Council:—The funds of the Certification Council shall comprise of:

(a) grants from the Federal Government;

(b) fee for grant and renewal of accreditation certificate: and

(c) fee, not exceeding test Rupees, for every certificate deposited in the repository.

(d) fines.

21. Functions of the Certification Council:—(1) The Certification Council shall perform such functions as are specified in this Ordinance or may be prescribed.

(2) Without prejudice to the generality of the foregoing sub-section the Certification Council shall:

(a) grant and renew accreditation certificates, to certification service providers, their cryptography services and security procedures;

(b) monitor and ensure compliance by accredited certification service providers with the terms of their accreditation and revoke or suspend accreditation in the manner and on the grounds as may be specified in the regulations;

(c) monitor compliance of accredited certification service providers with the provisions of this Ordinance;

(d) establish and manage the repository:

(e) carry out research and studies in relation to cryptography service and to obtain public opinion in connection therewith;

(f) recognize or accredit foreign certification service providers;

(i) make recommendations to an appropriate authority in relation to the matters covered under this Ordinance.

22. Application of Act XVII of 1996:—Notwithstanding anything contained in the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996), the Certification Council shall be exclusively responsible to grant, renew, suspend or revoke the accreditation to certification service providers, their cryptography services and security procedures:

Provided that, the foregoing provision shall not affect the applicability or operation of the provisions of the Pakistan Telecommunication (Re-organisation) Act, 1996 (XVII of 1996) to the telecommunication systems or telecommunication services, other than cryptography services, provided by the cryptography service providers.

23. Repository:—(1) The Certification Council shall establish and manage a repository for all accreditation certificates, certificates issued by accredited certification service providers and for such other information as may be specified in regulations made by the Certification Council.

(2) The Certification Council shall take appropriate measures to ensure the security of all information contained to the repository.

(3) All information contained in the repository shall be open to public inspection.

(4) Notice of suspension or revocation of any accreditation or of certificate issued by an accredited certification service provider, shall be posted in the repository within the prescribed time.

24. Grant of accreditation:—(1) The Certification Council may grant accreditation to certification service provider its cryptography services, electronic signature or advanced electronic signature and security procedures who complies with the criteria for accreditation specified in the regulations.

(2) The terms and conditions of the accreditation, including those relating to duration of the accreditation, renewal, suspension or revocation, shall be specified in the regulations.

(3) The fee for grant and renewal of the accreditation shall be as prescribed.

(4) The form and manner of proceedings for the consideration of application for grant, renewal, suspension or revocation of accreditation shall be specified in the regulations.

Provided that, the regulations shall provide for a transparent procedure with due regard to the right of hearing.

25. Certification practice statement:—(1) Each certification service provider, desirous of being accredited shall prepare and have at all times accessible a certification practice statement in such form and with such details, particulars and contents as may be specified to the regulations made by the Certification Council.

(2) Without prejudice to the generality of the foregoing, the regulations may provide for:

(a) prompt information to persons likely to be adversely affected by any event relating to the information system of the certification service provider or inaccuracy, invalidity or misrepresentation contained in a certificate;

(b) identification of subscribers.

(c) suspension or revocation of certificates;

(d) accuracy of information contained in a valid accreditation certificate.

(e) foreseeability of reliance on valid accreditation certificates; and

(f) deposit of certificates or notification of any suspension or revocation of any accreditation certificate or any other fact or circumstance affecting the certificate, in the repository.

(3) The certification practice statement shall be submitted to Certification Council for approval along with the application for accreditation.

(4) Any subsequent change in the approved certification practice statement shall be initiated and processed in such manner as may be specified in the regulations made by the Certification Council, and upon approval by the Certification Council, shall be incorporated in the certification practice statement;

(5) A copy of the certification practice statement shall be maintained at the office of the Certification Council and shall be open to public inspection

(6) Subject to such limitations as maybe specified in the regulations made under sub- section (1), a certification service provider shall, during the period of validity of an accreditation certificate published for reliance by any person be deemed to warranting to such person that:

(a) the certification service provider has complied with the requirements of this Ordinance, rules and regulations made under this ordinance; and

(b) the information contained in the certificate is accurate.

(7) The Certification Council may suspend or revoke the accreditation of a certification service provider for failure to comply with the provisions of this section:

Provided that, an order for suspension or revocation of accreditation shall be made in the manner specified in regulations made under sub-section (1) after providing reasonable right of hearing.

26. Decision of Certification Council:– All applications and matters coming before the Certification Council shall be decided through a speaking order, as expeditiously as possible but not later than ninety days except to extraordinary circumstances and for reasons to be recorded.

27. Appointment of offices, employees and advisers:—The Certification Council may appoint such officers, employees and advisers as it may consider necessary for the efficient performance of its functions on such terms and conditions as it may prescribe by the regulations.

(2) The Certification Council may establish regional or local offices as may be necessary for efficient performance of its functions.

CHAPTER 6
AMENDMENTS OF CERTAIN LAWS

28. Amendment of Act XVII of 1996:—(1) In the Pakistan Telecommunication (Re-organisation) Act, 1996 (XVII of 1996), clause (b) of subsection (2) of section 57 shall be omitted.

(2) Any provision in any licence issued by the Pakistan Telecommunication Authority under the aforesaid Act prohibiting the provision or use of cryptography services shall cease to have effect subject to provisions of this Ordinance.

29. Amendment of Presidential Order No. X of 1984:—For the purposes of this Ordinance, the Qanun-e-Shahadat Order, 1984, (P.O. No. 10 of 1984) shall be read subject to the amendments specified in the Schedule to this Ordinance.

30. Extension to electronic forms:– Notwithstanding anything contained in any other law for the time being in force, the expressions “attestation”, “books”, “books of accounts”. “certificate”, “charts”, “deed”, “document” “document of title” “execution”, “instrument”, “ledger”, “map”, “original”, “plans”,' publish”', “record”, “register”, “seal”, “signature”, “witnessing”, “words”,

"writing", or other words assuming paper or other tangible medium in relation thereto, shall, mutatis mutandis, extend to electronic forms thereof.

CHAPTER 7
OTHER LAWS AND JURISDICTION

31. Application to certain laws barred:—(1) Subject to sub-section (2), nothing in this Ordinance shall apply to:

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act,1881 (XXVI of 1881);

(b) a power-of-attorney under the Powers of Attorney Act, 1881 (VII of 1882);

(c) a trust defined to the Trust Act 1882 (II of 1882), but excluding constructive, implied and resulting trusts;

(d) a will or any form of testamentary disposition under any law for the time 'being to force; and

(e) a contract for sale or conveyance of immovable property or any interest in such property.

(2) The Federal Government after consultation with the provinces may by notification in the official Gazette and subject to such conditions and limitations as may be specified therein, declare that the whole or part of this Ordinance shall apply to the whole or part of one or more instruments specified in clauses (a) to (e) of sub-Section (1).

32. Application to acts done outside Pakistan:—The previsions of this Ordinance shall apply notwithstanding the matters being the subject hereof occurring outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons information systems or events within the territorial jurisdiction of Pakistan.

33. Overriding effect:—The provisions of this Ordinance shall apply notwithstanding anything to the contrary contained in any other law for the time being to force.

CHAPTER 8
OFFENCES

34. Provision of false information:— etc. by the subscriber—(1) Any subscriber who:

(a) provides information to a certification service provider knowing such information to be false or not believing it to be correct to the best of his knowledge and belief;

(b) fails to bring promptly to the knowledge of the certification service provider any change in circumstances as a consequence whereof any information contained in a certificate accepted by the subscriber or authorized by him for publication or reliance by any person, ceases to be accurate or becomes misleading, or

(c) knowingly causes or allows a certificate or his electronic signatures to be used in any fraudulent or unlawful manner,

shall be guilty of an offence under this Ordinance;

(2) The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.

35. Issue of false certificate, etc:—(1) Every director, secretary and other responsible officer, by whatever designation called, connected with the management of the affairs of a certification service provider, which:

(a) issues, publishes or acknowledges a certificate containing false or misleading information;

(b) fails to revoke or suspend a certificate after acquiring knowledge that any information contained therein has become false or misleading;

(c) fails to revoke or suspend a certificate in circumstances where it ought reasonably to have been known that any information contained in the certificate is false or misleading;

(d) issues a certificate as accredited certification service provider while its accreditation is suspended or revoked; shall be guilty of any offence under this Ordinance.

(2) The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.

(3) The certification service provider or its employees specified in subsection (1), shall also be liable, upon conviction, to pay compensation for any foreseeable damage suffered by any person or subscriber as a direct consequence of any of the events specified in clauses (a) to (d) of sub-section (1).

(4) The compensation mentioned in sub-section (3) shall be recoverable as arrears of land revenue.

36. Violation of privacy of information:— Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with imprisonment of either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both.

37. Damage to information system, etc:– (1) Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorized to do any of the foregoing shall be guilty of an offence under this Ordinance.

(2) Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance.

(3) The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees or with both.

38. Offences to be non-bailable, compoundable and cognizable.—All offences under this Ordinance shall be non-bailable, compoundable and cognizable.

39. Prosecution and trial of offences.—No Court inferior to the Court of Sessions shall try any offence under this Ordinance.

CHAPTER 9
MISCELLANEOUS

40. Limitation on liability of network service providers.—In the absence of intent to facilitate, aid or abet, a network service provider shall not be subject to any civil or criminal liability solely for the reason of use of his telecommunication system in connection with a contravention of this Ordinance by a person not subject to the direction or control of the network service provider.

Explanation.—Telecommunication system in this section shall have the meaning given thereto under the Pakistan Telecommunication (Re-organization Act, 1996 (XVII of 1996).

41. Immunity against disclosure of information relating to security procedure:—(1) Subject to sub-section (2), no person shall be compelled to disclose any password, key or other secret information exclusively within his private knowledge, which enables his use of the security procedure or advanced electronic signature.

(2) Sub-section (1) shall not confer any immunity where such information is used for the commission of any offence under any law for the time being in force.

42. Power to make rules:— The Federal Government may, by notification in the official Gazette, make rules to carry out the purposes of this Ordinance.

43. Power to make regulations:—(1) The Certification Council may, with the prior approval of the Federal government, make regulations to carry out the purpose of this Ordinance.

(2) Without prejudice to the generality of the sub-section (1), regulations may provide for:

(a) safety, control, or management of keys, passwords or other secret information relating to use of services of accredited certification service providers;

(b) standards, procedures and practices for time and date stamping;

(c) minimum qualifications of staff of accredited certification service providers;

(d) adequacy of facilities and equipment for secure and reliable operation:

(e) privacy and protection of data of subscribers;

(f) inspection of operations;

(g) cross-certifications, accreditation, recognition, bridge certification or other arrangements with certification service providers based in other countries;

(h) development of certification 'management system;

(i) reparation to subscribers for damage arising from negligence of certification service provider with conditions for and limits to liability;

(j) identification of areas of commerce or governance for use of certificates;

(k) standardization and technology relating to protocols, algorithm., interpretability of systems, applications and infrastructure for accredited certification service providers;

(l) form and contents of applications for accreditation;

(m) suspension or revocation of certification;

(n) suspension or revocation of accreditation;

(o) certificate profiles with mandatory and optional fields and extension fields, if any:

(p) certificate revocation and suspension list profiles with mandatory and optional fields, and extension fields (if any);

(q) retention of records by certification authorities and the repository;

(r) recommended code of practice for handling and storage of business information and records in electronic form; and

(s) regulation of access and audit trails.

44. Prior publication of rules and regulations:—(1) All rules and regulations proposed to be made by the Federal Government and the Certification Council under this Ordinance shall be published in the official Gazette and in at least one English and one Urdu daily with nationwide circulation, in draft form at least thirty days before the intended date of coming into operation.

(2) The Certification Council shall keep received of all comments received on the draft of the rules or regulations, and shall prepare a report thereon addressing each comment.

(3) The notification of the rules or regulations in their final form in the official Gazette shall be accompanied with a report of the Certification Council referred to in sub-section(2).

45. Removal of difficulties:—The Federal Government may, by notification in the official Gazette, make provisions for removal of difficulties in a manner not inconsistent with the provisions of this Ordinance.

SCHEDULE

(See section 29)

AMENDMENT IN QANUN-E-SHAHADAT ORDER, 1984 (PO. No. 10 OF 1984)

1. Amendment of Article 2. P.O. No. 10 of 1984.—In the Qanun-e-Shahadat Order, 1984 (P.O. No. 10 of 1984), hereinafter referred to as the said Order, in clause (1), after sub-clause (d), the following new sub-clauses (e) and (f) shall be added, namely:

"(e) the expression, "automated", "electronic", "information", "information' system", "electronic document", "electronic signature", "advanced electronic signature" and "security procedure", shall bear the meanings given in the Electronic Transactions Ordinance, 2002;

(f) the expression "certificate", where the context so admits, includes the meaning given to it in the Electronic Transactions Ordinance 2002."

2. Amendment of Article 30, P.O. No, 10 of 1984.—In the said Order, in Article 30, for the full stop at the end a colon shall be substituted and thereafter the following explanation shall be added, namely:

"Explanation.—Statements generated by automated information systems may be attributed to the person exercising power or control over the said information system."

3. Insertion of new Article 46, P.O. No. 10 of 1984.—In the said Order, after Article 46 the following new Article shall be inserted, namely:—

"46-A. Relevance of information generated, received or recorded by automated information system Statements in the form of electronic documents generated, received or recorded by an automated information system while it is in working order, are relevant facts.

4. Amendment of Article 59, P.O. No. 10 of 1984.—In the said Order, in Article 59—

(a) after the word "impressions" the comma and the words ", or as to authenticity and integrity of electronic documents made by or through an information system" shall be inserted; and

(b) for the words "are relevant facts" the words and commas "or as to the functioning, specifications, programming and operations of information systems are relevant facts" shall be substituted.

5. Amendment of Article 73, P.O. No. 10 of 1984.—In the said order, in Article 73, after the second Explanation, the following new Explanations shall be added, namely:

"Explanation 3.—A printout or other form of output of an automated, information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form if the automates information system was in working order at all material times and, for the purposes hereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material time.

"Explanation 4.—A printout or other form of reproduction of an electronic document, other than a document mentioned in Explanation 3 above, first generated, sent, received or stored in electronic form shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored.

6. Insertion of new Article, P.O. No. 10 of 1984.—In the said Order, after Article 78, the following new Article shall be inserted, namely:—

"78-A, Proof of electronic signature and electronic document. If, an electronic document is alleged to be signed or to have been generated wholly or in part by any person through the use of an information system and where such allegation is denied, the application of a security procedure to the signature or the electronic document must be proved."

7. Amendment of Article 85, P.O No.10 of 1984:—In the said Order, in Article 85, after clause (5), the following new clause (6) shall be added, namely:

"(6) certificates deposited in a repository pursuant to the provisions of the Electronic Transactions Ordinance, 2002."