Electronic Commerce

and

Cyber Crime

Laws of Pakistan

Jawad A. Sarwana

Abraham & Sarwana

Electronic Commerce and Cyber Crimes

1. **Introduction**

2. **Electronic Transaction Ordinance, 2002**

   - **Digital Signatures**
     - **Electronic Signatures (ES)**
     - **Advanced Electronic Signatures (AES)**

   - **Certification Service Providers (CSP)**

   - **Offences relating to ES, AES and CSP**

   - **Electronic Certification Accreditation Council**

   - **Protections against hacking, spyware, DoS, etc.**

   - **Extra Territorial Jurisdiction**

   - **International Certification Service Providers**

   - **Limitation on liability of Network Service Providers**

3. **Electronic Crimes Bill 2004**
   - **spoofing**
   - **cyber stalking**
   - **pornography**
   - **malicious code**
   - **spamming**
   - **And more. . .**

Highlights of ETO, 2002

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.

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.

Jawad A. Sarwana Abraham & Sarwana

IBM – Four **PAIN**'s of E-business

Privacy. E-business transactions are protected against access by attackers who seek to make copies of them or to insert fraudulent data into the process.

Authentication. Access to e-business applications and data is restricted to those who can provide the appropriate proofs of identity.

Integrity. E-business data and applications are protected in such a way that any effort to change them is detected and prevented.

Non-repudiation. The flow of data through an e-business application and the flow of transactions that drive the data are logged and reported in such a way that should a dispute arise about any transaction, proof of what actually happened can be produced.[1]

[1] See http://www-106.ibm.com/developerworks/library/s-pain.html

PAKISTAN's PAIN

Privacy – Section 36.

Authenticity means in relation to an electronic document or electronic signature, the identification of and attribution to a particular person or information system. (Section 2(f), ETO, 2002).

Integrity means 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. (Section 2(q), ETO, 2002)."

Non-repudiation ?

Digital Signature

"Electronic Signature (ES) 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 the authenticity or integrity or both. (emphasis added)"

"Advanced Electronic Signature (AES) means an

Electronic Signature which is either

(i) unique to the person signing it, capable of identifying such person, created in a 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.

No PAIN, No Gain

Jawad A. Sarwana

Abraham & Sarwana

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.

"Subscriber" means a person who subscribes to the services of a certification service provider

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 (l) 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.

The certification service provider or its employees specified in sub-section (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.

Electronic Certification Accreditation Council

Five Members

1	A Telecommunication Engineer with atleast seven years of experience in the field of cryptographic services.
2	Professionals or Academics with atleast seven years of experience in the field of Information Technology
1	Administrative background with atleast seven years of experience in a private or public organization
1	An Advocate with atleast seven years of experience and adequate knowledge of laws relating to information technology and telecommunications

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 authorized to gain access, as aforesaid,

shall be guilty of an offence under this ordinance

punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees or with both."

Damage to Information System etc:

(1) Any person who

does or attempts to do any act with intent

to alter, modify, delete, move, generate, transmit, or store any information

through or 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.

(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 authorized to do any of the foregoing,

shall be guilty of an offence under this ordinance.

(3) The offences under sub sections (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.

Extra Territorial Jurisdiction

International Certificate Service Providers

Liability of Network Service Providers for Actions of Subscribers

Jawad A. Sarwana

Abraham & Sarwana

Electronic Crimes Bill 2004

Phreaking	Pakistan Telecommunication Re-organization Act, 1996
Spamming	Electronic Crimes Bill 2004 Section 16
Spoofing	Electronic Crimes Bill 2004 Section 17
Cyber Terrorism	Electronic Crimes Bill 2004 Section 20
Waging Cyber War	Electronic Crimes Bill 2004 Section 21
Electronic Fraud	Electronic Crimes Bill 2004 Section 8
Electronic Forgery	Electronic Crimes Bill 2004 Section 9

Jawad A. Sarwana

Abraham & Sarwana