Journal of Law & Social Studies (JLSS)
Volume 5, Issue 2, pp 307-321
www.advancelrf.org

An Appraisal of Pakistan's Electronic Transaction Law and Certification Service Providers' Accreditation Regulations

Waqas Rafiq
Lecturer,
Department of Law, University of the Punjab, Gujranwala Campus, Punjab.
Email: waqas.rafiq@pugc.edu.pk

Muhammad Bilal
(Corresponding Author)
Associate Professor,
Gillani Law College, B. Z. University, Multan.
Email: mbilal@bzu.edu.pk

Ghulam Mustafa
Assistant Professor,
Department of IT, University of the Punjab, Gujranwala Campus, Punjab.
Email: gmustafa@pugc.edu.pk

Abstract

This paper aims to evaluate the current legal landscape in Pakistan concerning contracting practices conducted through modern forms of communication. The advancements in information technology, electronic processing, and communication have paved the way for paperless and automated trade. Consequently, the effectiveness of traditional paper-based communication in business transactions is being challenged, with electronic alternatives gaining prominence. In response to global and national legislative initiatives, Pakistan has enacted the Electronic Transaction Ordinance 2002 and Certification Service Providers' Accreditation Regulations 2008. These laws aim to legally recognize electronic documents and signatures while providing a framework for accrediting certificate providers.The study adopts a black letter approach, conducting a descriptive and critical analysis of primary legal sources while considering concerns raised in secondary sources. Overall, this research sheds light on the current state of laws governing e-contracting practices in Pakistan, highlighting the need for ongoing adaptation and improvement to accommodate the evolving landscape of electronic transactions. The findings reveal that Pakistan's legal response offers a strong foundation for the future development of e-commerce and e-government. However, certain amendments are needed to align with current trends in international e-commerce laws.Pakistan may improve its legal framework and encourage e-commerce and e-government by accepting these reforms and making appropriate amendments.

Keywords: Certification Service Providers' Accreditation Regulations, E-commerce, Electronic Documents, Electronic Signatures, Electronic Transaction Ordinance, Pakistan

Introduction

The evolution of technology has altered the manners in which the world operates. The manners in which businesses and non-profit organizations conduct business and other social activities have changed drastically as a result of modern technology, particularly internet access (Haileyesus, 2021). Historically, paper documents and ink-based signatures were the norm for commercial transactions. Numerous legal standards rely on the existence of written records and paperwork, signed documents, original documentation, physical currency, negotiable instruments, and in-person dialogues (Basu & Jones, 2003). However, improvements in information technology, computer processing, and communication are making it possible to do business without paper and with machines. Because of this, the usefulness of paper and other physical forms of business communication has been challenged and the use of technological options is being supported instead.

Nevertheless, this development has raised concerns about the recognition, validity, admissibility, effect, proof and enforceability of electronic documents, records, communications, and transactions in the legal domain. The response consists of a multiplicity of global and national legislative initiatives. Pakistan is not an exception, as not only has it enacted the Electronic Transaction Law (ETL), but its regulatory body has also promulgated regulations for incidental matters such as certification provider accreditation, etc. This research's operational framework is comprised of the following sections: the second section examines electronic documents, electronic signatures, certification authorities, and certificate providers from a theoretical standpoint. In the third section, important legislative developments of ETLs at the global and national levels that inspired their adoption in Pakistan are examined. Pakistan's Electronic Transaction Ordinance, 2002, and Certification Service Providers' Accreditation Regulations, 2008, are examined in the fourth section of this study, which constitutes the bulk of the research's analysis. The article concludes with suggestions for improvement and a conclusion. In this study, doctrinal legal research was used to obtain a deeper understanding of the investigated topic. The primary legal sources, such as statutes, treaties, rules, and regulations, were consulted for this study. In order to collect in-depth information, evaluate the data effectively, and meet the study's objectives, secondary data in the form of research publications and journals were also evaluated.

Electronic Documents, Electronic Signatures, Certification Authority and Certificate Providers

Electronic Documents

In contrast to paper documents, electronic documents consist of bit sequences and are stored on digital media (Pun et al., 2002). Consequently, they possess two distinct characteristics. Firstly, they can be duplicated without quality loss. As a consequence, there is no such thing as an “original copy” of electronic documents, as each duplicate generated is identical to the original and is of equal quality. Secondly, they are seamless. They can be modified readily and leave no trace. Any portion of an electronic document can be meticulously extracted and pasted into another without detection. The generated documents will appear identical to all other electronic files.

These two characteristics make electronic document forgery considerably easier than forgery of paper documents. There are typically no discernible differences between a forgery and a genuine electronic document, making it possible for anyone unfamiliar with digital technology to be duped. Therefore, the authenticity of electronic documents is a significant obstacle in determining the validity of contractual relationships in the digital environment, and drafters of legislation governing electronic commerce must address this issue. Reed (2001) has outlined three criteria for determining the veracity of an electronic communication's record: (1) the integrity of the record; (2) the identity of the sender; and (3) the attribution of the communication to the sender.

Electronic Signatures

Signatures are widely acknowledged as a requirement for the authenticity of all business and government documents (Arslan, 2015). Signatures are essential for linking the text of a signed document to the signatory and demonstrating the parties' intent in embracing the contents of a signed document. Various technologies make it possible for electronic signatures to fulfill the responsibilities linked to handwritten signatures (Kim, 2019). Electronic signatures may consist of digitized pictures of handwritten signatures, requests sent via email with distinct URLs, passwords generated through phone verification, company IDs, and the signatory's biometric features, such as retina scans, face geometry, and fingerprints, which are all examples of biometric traits. Different electronic signature methods provide varying levels of assurance regarding the signer's identity and the signature's authenticity. Distinctive signature methods call for different technologies and provide differing levels of protection. It may be as easy as typing one's name or initials into a computer's text box and pressing the "I agree" button, or it could include complicated technology like public key encryption or biometric identification. In contrast to biometric signatures, which are tied to a particular human being, electronic signatures are connected with a code, "cryptographic key", or other type of digital data rather than a person.

Digital Signatures

The first notable approach for "electronic signatures" also known as "digital signatures" may be credited to cryptographic innovations in the 1970s, including the invention of "public key cryptography" (PKC) or asymmetric encryption (Diffie, 1988; Mason, 2016). The creation of "digital signatures" necessitates a series of operations requiring substantial processing power and computational capacity for encryption and decryption. PKC employs two mathematically related keys for encoding and decoding. The "private key" is a secret number that can only be used by the person who signed the electronic communication, as determined by its mathematical link to the matching public key. Digital signatures can only be guaranteed to be secure if they use this two-key technique in which both keys are equally important. While only the signer has access to the secret "private key," anybody may access the publicized "public key" and use it to verify other people's signatures.

Public key infrastructure (PKI) and cryptographic technologies have advanced concurrently with the development of digital signatures (Haileyesus, 2021). The primary purpose of PKI and cryptography is to provide digital signature consumers with security and confidence. PKI includes the hardware, software, individuals, and procedures involved in the creation, administration, storage, distribution, and revocation of keys and digital signatures (Adams & Lloyd, 1999).

The Role of Certification Authority

To confirm the authenticity of a proposed signature, an additional step is required since a "public-private key pair" is not tied to a single person by definition (Kim, 2019). The "Certification Authority" (CA) serves as a trustworthy third party between the signer and the recipient of the signed communication (the "reliant party") since there is no preexisting trust between the two parties. CAs may be overseen by any number of public, private, non-profit, and governmental organizations. There is usually more than one CA in a national PKI, albeit in certain places only CAs officially acknowledged by the government are permitted to function.

A digital version of the certificate is created by the CA. Digital signatures and the messages they secure may be verified by the certificate's issuer, who can also attest to the signer's identity. Assuming the certificate was issued legitimately and has not been revoked by the CA, the relying

party acquires the "public key" indicated in the certificate and uses it to verify the identity of the signer and the authenticity of the signed communication.

Hierarchical and peer-to-peer are the two prevalent PKI frameworks (Satizábal et al., 2006). The hierarchical model is the most popular among online communities. (Albarqi et al., 2015). In a hierarchical PKI setup, everyone starts their certification processes using the public key of the CA. Instead of providing certificates directly to users, the CA grants licenses to certificate providers, who then distribute certificates to users. In a hierarchical approach, confidence relationships are unidirectional, which simplifies the creation of certification processes (Satizábal et al., 2006). Since the peer-to-peer paradigm lacks a top-down link, it operates independently in the absence of a higher CA. CAs demonstrate their independence through peer-to-peer cross-certification.

Accreditation of Certificate Provider

The eligibility of a certificate issuer is one of the primary concerns that drafters of electronic commerce legislation must address (Haileyesus, 2022). Certificate providers are not immune to failure; rather, they are susceptible to failure for a number of reasons (Smith & Kiefer, 1999). For instance, they could fail due to sloppy use of PKI mechanisms, negligent certification procedures, unjustified revocation or suspension of a certificate, faulty software, or even insolvency. States must establish a balance between two competing interests when enacting electronic validation laws: the desire to prevent unnecessary, heedless, or excessively stringent regulations and the desire to ensure the existence of appropriate regulations to avoid and rectify any failures.

In order to reconcile these competing interests, a law governing electronic authentication must regulate the who and how of certificate providers. There are many proponents and supporters of the licensed and controlled certificate provider system. One of its many uses is speeding up and improving the reliability of existing financial dealings. Second, if the parties ever get into a business disagreement, it may help clear things up and provide them a leg to stand on legally. By removing ambiguity, it enhances the customer's confidence in an electronic transaction. Fourthly, it safeguards consumers. Lastly, it can expand the authority to control the actions of the certificate provider (Blythe, 2006).

Legislative Developments of Electronic Transaction Laws

On 9th of March 1995, the state of Utah passed the "Utah Digital Signature Act 1995," first ETL in history. This law was technology-specific since it only recognized PKC-based digital signatures from CAs as equivalent to handwritten signatures (Richards, 1998). A little over six months later, California approved its own technology-neutral ETL and adopted a more adaptable strategy (Srivastava, 2012). This law did not differentiate between electronic and digital signatures, recognizing as a digital signature anything that could be used in lieu of a traditional signature in an electronic setting. Nonetheless, "Florida's Electronic Signature Act of 1996," enacted on May 31, possibly among the first ETLs to distinguish between electronic signature and digital signature. The Act established guidelines for digital signatures and gave substantial backing to the technology. In 1996, the "American Bar Association" (ABA) issued a comprehensive report on digital signatures titled "Digital Signature Guidelines," which indicated further advancements in the field of electronic signatures. To facilitate international electronic trade and to provide credibility and transparency to digital agreements, the United Nations (UN) has introduced a number of proposals. Since 1984, the "United Nations Commission on International Trade Law" (UNCITRAL) has been constructing a comprehensive legislative framework to regulate electronic commerce. This legislative endeavor resulted in the implementation of "Model Laws on Electronic Commerce" (MLEC) and "Model Laws on Electronic Signatures" (MLES) by UNCITRAL in 1996 and 2001, respectively. Paper-related terms such as "writing,""signature," and "original" are functionally

equivalent in the MLEC. The objective of the Model Law is to provide national legislators with a model of universally recognised laws in order to reduce legal barriers and develop the legal environment for e-commerce. It endeavors to promote the global harmonization of national legal systems with the purpose of making electronic communication easier to use(Khan, 2012).

Whereas the MLES seeks to increase legal clarity regarding the use of electronic signatures in accordance with the MLEC Article 7 which contains an adaptable concept. It establishes a presumption that electronic signatures should be recognized as equivalent to handwritten signatures, provided that certain technological reliability requirements are met. In addition, it takes a technology-neutral stance and avoids endorsing any particular technological solution. This Model Law aims to encourage the global harmonization of regulations governing certifying agencies and electronic signatures. It establishes fundamental criteria in order to validate digital signatures from other jurisdictions and provides guidelines for the behavior of various parties interacting with electronic signatures. (Kim, 2019) The Model Laws have been effective in uniting nations with disparate economic standings and legal systems.

The first global convention regulating e-commerce was the “United Nations Convention on the Use of Electronic Communications in International Contracts” (ECC), which was enacted by the UN General Assembly in 2005 and particularly regulates “international” contracts conducted via electronic technology. The MLEC lacks some key provisions that are included in the ECC. (Boss, 2009). The Convention may have provided an opportunity for the global harmonization of national ETLs because it is a “hard” law binding on ratifying governments, but as of now, only 18 nations are members of the ECC, and Pakistan is not among them.

Conceptual Approaches Towards ETLs

Despite UNCITRAL's efforts to harmonize the rules, the past several years has witnessed an explosion of state legislative and regulatory actions in the arena of electronic authentication (Khan, 2012). In an effort to capitalize on and regulate this new technology, legislative and regulatory entities around the globe have adopted three distinct approaches: (1) prescriptive, (2) minimalist, and (3) two-tiered (Fischer, 2001).

The Prescriptive Approach

To satisfy the regulations for effective electronic signatures, this paradigm requires the use of a specific technique known as asymmetric cryptography and supports digital signatures that have been generated and validated using PKC (Kim, 2019). In addition, it imposes explicit practical and monetary constraints on CAs, defines the responsibilities of key owners, and specifies the circumstances under which an electronic signature can be trusted. The prescriptive regulation places operational and financial obligations on CAs in order to guarantee the authenticity of the PKI, as they play a key role in maintaining it. Although Germany, Italy, and Argentina are some examples of countries with civil law systems that have chosen to use a prescriptive approach, Malaysia and India have also embraced this method (Khan, 2012).

One of the controversial aspects of the prescriptive method is that there is an imbalance in the allocation of risk among users of digital signatures. Protecting the “private key” from being used dishonestly or in any other way that violates the agreement is the signatory's main duty under the law. In addition, the signatory has an unlimited responsibility in the event that they fail to take adequate precautions to protect the “private key,” but Cas, that have been granted a license by the relevant state authority, are often free from liability (Biddle, 1997). While mandating the use of digital signatures does make users safer, the benefits of doing so may be offset by the fact that

digital signatures are more difficult to use, more burdensome financially, and less adaptable to the technology used in other nations (Roland, 2001).

The Minimalist Approach

The law that sets up this framework, on the other hand, makes no assumption about, or mandates a specific electronic signature technology (Kim, 2019). Any technology capable of executing the basic purposes of a signature, i.e., recognizing the signatory and demonstrating the signatory's intent to sign, may be used to create legally valid and enforceable signatures. Consequently, the vast majority of electronic signatures are deemed equivalent to text signatures. Although parties are free to use electronic methods by mutual consent, certain categories of transactions may be required to remain paper-based by law. Khan (2012) argues that traditional common law nations such as "Canada, the United States, the United Kingdom, Australia, and New Zealand" have adopted a more minimalist approach. However, this view is flawed because it ignores the fact that digital signatures are inherently more secure than other types of electronic signature (Blythe, 2009).

The Two-Tiered Approach

This structure is a combination of the two concepts listed above (Kim, 2019). Critical to this context is the law's limited technical neutrality, which sets low requirements for technical criteria to provide minimal legal recognition for a broad range of electronic signatures while providing additional legal advantages (e.g., presumption of validity) to advanced electronic signatures employing specified technologies that meet stricter standards. China, Colombia, European Union, South Korea, Mexico, Switzerland and Norway are among the nations that adopt this method. Not only are such laws superior to alternative legislative approaches because they are more adaptable and receptive to the most recent technological advancements, but they also provide people the assurance of the law needed to trust electronic signatures (Fisher, 2001). However, opponents claim that it doesn't give market forces any discretion, overprotects specific technology at the cost of innovation, and tant amount to excessive government control.

Pakistan's Electronic Transaction Ordinance 2002 and Certification Service Providers' Accreditation Regulations, 2008

The Government of Pakistan approved its IT Policy in 2000 and established an IT Law Forum comprised of the country's prominent legal professionals working in various sectors of law linked to information technology to create laws relevant to electronic transactions (Khan, 2012). The forum conducted multiple discussions with the financial and legal communities, and after analysing UNCITRAL model laws, reviewing various electronic authentication implementation approaches, legislative models, and best practice guidelines drafted the ETL for Pakistan. The President of Pakistan promulgated the Electronic Transaction Ordinance (ETO) and it came into force with effect on 11th September, 2002 after publication in the Official Gazette. The essence of the ETO as encapsulated in its preamble is twofold: (1) "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and (2) to provide for the accreditation of certification service providers." When other Pakistani laws come into conflict with the ETO, the ETO will take precedence (ETO, s 33).

ETO's Chapter V i.e. sections 18-27 deal with the CA which is designated as Certification Council (CC) and it's complete name is Electronic Certification Accreditation Council as per section 2(i). The CC is entrusted with regulating Certification Service Providers (CSPs) and as a result, a hierarchical PKI architecture is established, with the CC designated as the CA. The CSPs are controlled under the ETO which specifies the conditions that must be met to become a CSP and provides a compulsory system of CSPs accreditation. Additionally, the CC has promulgated the

"Certification Service Providers' Accreditation Regulations, 2008" (CSPAR) under Section 43 read with Sections 21, 22, 24 and 25 of ETO. The CSPAR provides for, inter alia, the terms and conditions, duration, fee, and procedures for the deliberation of requests for "grant, renewal, suspension or revocation of accreditation".

Exclusions

The standard list of exclusions in international E-commerce legislation (which prohibit the use of electronic documents) is progressively being reduced (Blythe, 2010). In contrast, Pakistan has a list of exclusions which prohibits the use of electronic documents in the case of trusts, powers of attorney, wills, negotiable instruments and agreements for the sale or transfer of immovable property(ETO, s.31). However, the federal government, after consultation with the provinces, may authorize the application of the ETO to these instruments by notification.

E-Government

Despite the list of exclusions, the federal and provincial legislatures, governments, statutory bodies, Supreme Court, and High Courts are persuaded to receive, issue, and preserve documents in electronic form or to carry out monetary transactions without conferring statutory rights on citizens (ETO, s. 16). Consequently, these authorities may recognize the validity of electronic documents and electronic forms for (a) documents filing, creation, or retention; (b) the issuance of certification, permit, license, or sanction; or (c) the mode and means of payment, procurement, or transaction. Nonetheless, each appropriate authority has the option to enact regulations regarding the format and presentation of electronic documents, the type of security procedure, the format and presentation of electronic signatures, the function of CSPs, etc.

Legal Recognition and Presumptions regarding Electronic Documents

The term "electronic document" has been defined as including "documents, records, information communications or transactions in electronic form" (ETO, s. 2(m)). Whereas the term "electronic" includes "electrical, digital, magnetic, optical, biometric, electro-chemical, wireless or electromagnetic technology" (ETO, s. 2(l)). No document, etc. shall be denied "legal recognition, admissibility, effect, validity, proof or enforceability" merely because it is in electronic format and the attesting witnesses are absent (ETO,s. 3). The availability of a document or other item in an electronic format and available for future use will meet the need that it be in written form under applicable law (ETO,s. 4).

The ETO permits and accepts electronic document submission. If the presentation or preservation of a document or other item in its original form is mandated by law, that need is fulfilled if: (1) one may be certain of their veracity from the time of creation to final form; and (2) they can be presented in a legible form (ETO, s. 5). The criterion for determining the document's integrity is whether it has remained intact and unaltered. When evaluating the requirement for assurance reliability, the intent behind the creation of the document and any other pertinent factors will be considered.

If a law needs the preservation of documents etc., this obligation is met by preserving the documents etc. in electronic format, provided that: (1) their contents are accessible for future reference; (2) their format and contents are either identical or capable of depicting exactly as "generated, sent or received" initially; and (3) information regarding their source, target, time and date of generation, transmission and reception is preserved (ETO, s.6) . If any law needs or authorizes the submission of certified copies of records, printouts, or other forms of exhibition, "electronic documents" may be introduced as certified copies if the requirements of such law are met along with the method of verification outlined by the appropriate authority (ETO, s. 12).

Legal Recognition and Presumptions regarding Electronic Signatures

The ETO has followed "two-tier" approach (Khan, 2015) as it recognizes two kinds of digital signatures: (1) "electronic signature" and (2) "advanced electronic signature". The expression "electronic signature" refers to any electronically applied "letters, numbers, symbols, images, characters" or their combinations that are incorporated into or connected to an electronic document with the goal of establishing the document's genuineness, integrity, or both (ETO, s. 2(n)). Whereas, the term "advanced electronic signature" refers to an "electronic signature" that is either (i) peculiar to the individual who is affixing it, with the ability to identify such person, built in a way or employing a means solely under the direction of the individual affixing it, and linked to the "electronic document" in such a way that any later modification in the "electronic document" is detectable; or (ii) supplied by an accredited CSP with the ability to establish genuineness and integrity of an electronic document (ETO, s. 2(d)).

If a law necessitates a person's signature to be attached to a paper document, this need will be satisfied by an "electronic signature" or "advanced electronic signature" affixed to an electronic record (ETO, s. 7). The proof an electronic signature can be accomplished by any method used to confirm that the "electronic document" was signed by the intended signer with the intent to confirm its accuracy or genuineness, or both (ETO, s. 8).

The ETO has provided the advanced electronic signature with enhanced sanctity by attaching rebuttable presumptions as: (1) the electronic document bearing it is valid and possesses integrity; or (2) (a) it is the "signature" of the intended originator, (b) it was attached to the "electronic document" for the purpose of signing or approving it, and (c) the "electronic document" has not been altered after its attachment. (ETO, s. 9).

Electronic Contract Rules

Attribution of Communications

The addressee of an electronic communication is permitted to assume that it has emanated from a particular originator if: (a) the originator send the communication or (b) the originator's agent send the communication or (c) the originator's computerized information system send the communication and (d) the addressee has no cause to doubt the electronic communication's authenticity or (e) in the absence of circumstances warranting exercise of reasonable care by the addressee regarding knowledge of unauthentic messages (ETO, s. 13). However, the originator and the addressee may agree to change these regulations.

Acknowledgment of Receipt

When the originator of an electronic communication specifies that it is contingent on receiving an acknowledgment, the message is not considered sent until the acknowledgement is received (ETO, s. 14). When the originator and addressee have not agreed on the precise format or mode of the acknowledgment, it may be provided in one of two ways: (a) any message delivered by the recipient—automated or not; or (b)any action done by the recipient—enough to prove to the sender that they received the message electronically. Nonetheless, the sender and the recipient can agree to modify these rules.

Time and Place regarding Dispatch and Receipt

When an electronic communication reaches a computer network that is not within the sender's control, it is considered to have been transmitted (ETO, s. 15).The electronic message is assumed to have been received at the time when: (1) it enters an IT system nominated by the addressee; or

when it is retrieved by the addressee where it enters such an IT system other than the one nominated by him; and (2) it enters an IT system of the addressee in case no IT system is nominated by him.

An electronic communication is considered to have been transmitted or received at the place of residence or business of the originator and addressee, respectively. However, if the originator or the addressee has multiple locations of business, the one with the closest tie to the underlying transaction is used; otherwise, the primary location of business is used. In case if they do not have a location of business, then "usual place of residence" is used. When referring to an incorporated body, "usual place of residence" refers to the location of its incorporated. However, the originator and the addressee may agree to change these regulations.

Regulation of Certification Service Providers

Functions of Electronic Certification Accreditation Council

Because CC is a government body, it can instill trust in CSPs and can also encourage the use of digital signatures by instilling confidence. Hence, adopting the hierarchical PKI architecture is a wise decision for Pakistan, whose overall technical growth is limited. Section 21 provides the basic functions of the CC which, inter alia, are to: (1) granting and renewing accreditation certificates to CSP's for cryptography assistances and security practices; (2) monitoring and ensuring obedience by accredited CSPs with the terms of their accreditation; (3) revoking or suspending accreditation; (4) creating and administering the repository; (5) conducting research and studies on cryptography services and solicit public opinion on the subject; (6) recognizing or accrediting foreign CSPs; (7) promoting uniform standards and practices; and (8) providing advice to concerned persons and making recommendations to appropriate authorities.

Repository

The CC is responsible for creating and maintaining a database that contains information such as CSP certificates, notifications of suspension or revocation, and accreditation certificates (ETO, s. 23). The CC is responsible for guaranteeing the security of the repository's information, which must be publicly accessible.

Accreditation of Certification Service Providers

According to section 17 of ETO a valid accreditation certificate issued by the CC is compulsory for any person to act as an accredited CSP. However, it is provided that this restriction shall not obstruct or limit the entitlements of any CSP to participate in the provision of certification services due to non-accreditation. As per section 24 the CC is authorized to grant accreditation to CSPs for "cryptography services, electronic signature or advanced electronic signature and security procedures" subject to compliance of accreditation standards stated in the regulations. The accreditation is valid for one year from the issuance of Accreditation Certificate (CSPAR, r. 11). The CC must decide upon all Accreditation Certificate grant and renewal applications within ninety days; however, the CC may reject or defer any application for reasons to be recorded in writing (CSPAR, r. 12).

Eligibility Requirements

Any person desirous of being accredited as CSP must submit application at the first stage to the CC with following information and documents (CSPAR, r. 4): (1) a Certification Practice Statement (ETO, s. 25); (2) a declaration showing the details of certification services to be provided; (3) a statement showing honesty, privacy, authenticity and protection of information and information system; (4) a statement indicating that two employees having a minimum of two years' experience

working in relation to the certification services; (5) the names of other persons and Trusted Persons employed by the Applicant for the purposes of carrying out the business or services; (6) a declaration of anticipated certification technology, risk management, disaster recovery, management, system manual or any operations to be outsourced; (7) a copy of refund policy clearly stating the manner of refund of fees to the subscribers in case the CSP discontinues its business for any reason; (8) certified copies of the registration documents, financial audit report and current statutory filings before the concerned authorities; and (9) a declaration of solvency.

All applicants at second stage of accreditation grant or renewal applications shall provide the complete and final Audit Report in pursuance of Accredited Certification Service Provider's Audit Regulations, 2008. It shall also provide an undertaking to submit proof of insurance for liability of loss not less than Rs. 10 M for claims against errors or omissions on by the Applicant, its officers or employees and an undertaking to submit a performance bond or a Banker's guarantee in favour of the CC for an amount of Rs.10 M (CSPAR, r. 4(6)). The said performance bond or banker's guarantee may be used to cover liabilities and rectification expenditures attributable to the negligence of the certification authority, its officers, or employees, as well as to cover the costs related to the discontinuation or transfer of accredited CSP's operations.

Effect of Accreditation

The Accredited CSP shall publish and make online publicly accessible and available the statements concerning its liabilities, limitations on liability, its rights and obligations, reliance limit of each type or classes of certificates that it issues (CSPAR, r. 14). It shall immediately notify any incident that adversely and materially affects the validity of the whole or any part of its information system or facility to the CC, its subscribers and relying parties and shall take immediate action to address the incident (CSPAR, r. 15). It shall have the right to check the identification of the subscriber from the National Data Registration Authority, in case of Company from the Securities and Exchange Commission of Pakistan and in case of Partnership concern from the relevant registration authorities before issuance of certificate to any subscriber (CSPAR, r. 16). It shall establish and maintain a subscribers' directory available 24/365 (CSPAR, r. 17). It shall be deemed warranting to any person relying on an accreditation certificate published that the CSP has fulfilled the requirements of ETO and related delegated legislation and the correctness of the info in the certificate (ETO, s. 25(6)).

Suspension, Revocation, Discontinuation and Their Effect

The CC has the power to suspend or revoke the accreditation of a CSP in case it fails to observe the provisions of ETO (ETO, s. 25(7)). However, the provision of prior show cause notice and reasonable right of hearing is compulsory before such order. The grounds of suspension (CSPAR, r. 18) are: (a) non-compliance of CSPAR; (b) non-compliance with the Audit Regulations of the CC; (c) furnishing of wrong information; (d) commission of breach of its Certification Practice Statement; (e) compromise of digital certificates, key pair, password due to the negligence of the Trusted Person; (f) failure to update or upgrade the repository; (g) use of expired digital certificate or non-archival of expired digital certificate in the repository; (h) non-payment of requisite fee for issuance of each digital certificate; (j) failure to supply the clients information when demanded by the Council or any investigating authority; (k) failure to submit quarterly list of clients and number of certificates issued; and (I) failure to report to the Council regarding any change in the constitution of the company, partnership and any other entity or change in the Trusted Persons.

However, as an alternative the CC may, while at hearing, without suspending the accreditation charge and accept payment of such fine which it deems proper in the same hearing and thereafter

may award reasonable time to the accredited CSP for rectification of the breaches, errors and omissions (CSPAR, r. 18(2)).

The CC may revoke Accreditation Certificate on the following grounds (CSPAR, r. 19): (a) application for renewal has not been made in accordance with prescribed form and manner and within prescribed time; (b) upon concealment of material facts and such information which may affect its business operations and method of conducting business in provision of cryptographic services to its subscribers in contravention of the ETO, the CSPARs and its Certification Practice Statement; and (c) breach, errors or omissions have not been rectified despite the direction of the CC. Additionally, the CC may revoke the accreditation on any other ground which amount to either gross negligence or material deviation from Certification Practice Statement (CSPAR, r. 19(2)).

The accredited CSP may discontinue to act and operate as CSP with the prior approval of the CC and after making arrangements of re-subscription of its subscribers to another accredited CSP (CSPAR, r. 22). The said CSP must comply the conditions like: (a) ninety days prior written notice to the CC; (b) sixty days prior advertisement in the daily newspapers; (c) sixty days prior notice to the CC, subscribers and cross certifying CSPs of each un-revoked or un-expired digital signature certificates issued by it; (d) revocation of all Digital Signature Certificates; (e) a reasonable effort ensuring that discontinuation causes minimal disruption to its subscribers and relying persons; (f) reasonable arrangements for preserving the records for 7 years; (g) payment of reasonable compensation to the subscribers, not exceeding the cost of new certificates of same validity period from identical certification service provider; (h) destruction of the certificate signing data and confirmation of its date and time to the CC at the time of completion of notice period; and (i) surrender the original Accreditation Certificate to the CC.

The accredited CSP if opts to transfer all of its certificates to another accredited CSP shall apply for issuance of no objection certificate from the CC and approval by furnishing the following: (a) a fee as detailed in Schedule I; (b) a certified copy of the agreement concluded between the transferee and transferor accredited CSPs; and (c) a proof in original that it has discharged all the financial obligations in favour of the CC. The CC may issue no objection certificate and accord its approval for transfer after its satisfaction of and fulfillment of the above conditions. However, every accredited CSP must ensure archiving of all issued certificates, maintaining systems to access such certificates and retaining records and logs of such archive up to 7 years. However, any person aggrieved from any order passed by any authorized officer or committee of the CC may prefer an appeal within 30 days to the CC (CSPAR, r. 31).

Liability of CSPs

Certification service is all about provision and authentication of information, as opposed to the sale of goods and other services (Smedinghoff, 1998). Certificate providers who issue digital certificates will be held accountable for the information provided on the digital certificate since it is meant to be relied on by parties in a specific matter. Therefore, a certificate provider's top priority is the accuracy of the issued certificates.

Section 35 of the ETO specifies the criminal liability of every director, secretary, and other responsible officer of a CSP who issues a false certificate. It is punishable for 7 years imprisonment, or a 10 million rupees fine, or with both. The offence of issuing false certificates encompasses the following acts or omissions: (a) issuing, publishing, or acknowledging a certificate enclosing dishonest or deceptive information; (b) failing to withdraw or suspend a certificate containing false or misleading information after such knowledge; (c) failing to revoke or suspend a certificate being obvious that any information contained in the certificate is inaccurate or deceptive; and (d) issuing a certificate as an accredited CSP during suspension or revocation of accreditation.

The CSP or its above-mentioned employees, when convicted, additionally must be liable to pay damages for any probable loss suffered by anybody or subscriber as a direct outcome of any of the above-mentioned events. The said compensation is recoverable as arrears of land revenue. Moreover, CSPAR's regulation 29 make CSPs and non-accredited CSPs having mutual cross certification arrangements with the accredited CSPs liable to pay damages for negligence to the subscribers and other relying person. Though, the civil liability of CSP is limited to Rs. 10 million as discussed above under CSPAR, r. 4(6), but the aggrieved party have the right to seek its remedy through court of competent jurisdiction for recovery of damages. Therefore, damages for loss of profits, pain, and suffering and in the nature of punitive (Osty & Pulcanio, 1999) are still recoverable by the suffering parties.

Additionally, according to CSPAR's regulation 28, the CC may impose a fine up to Rs. 15,000/- or the CC will lodge a criminal complaint against Accredited CSP for fraud or misrepresentation who contravenes the provisions of CSPAR by furnishing a wrong information in the application and gets accreditation. Further, if an accredited CSP commits any gross negligence or fails to provide an information required by these Regulations, the Council may impose a fine up to Rs.50,000/-.

Liability of Subscribers

A "subscriber" is a person, who takes to the services of a CSP (ETO, s. 2(y)). ETO's section 34 stipulates criminal liability for any subscriber who is involved in the provision of false information. It is punishable for 7 years imprisonment, or a 10 million rupees fine, or with both.

The acts or omissions which are designated as the offence of provision of false information include: (a) providing information to a CSP with the knowledge of its being false or not believing in its correctness to the best of his awareness and conviction; (b) failing to immediately intimate a CSP any modification in circumstances as a result of which any information in the subscriber's certificate no longer remains correct or becomes deceptive; or (c) willfully causing or allowing the use of his electronic signatures or certificate in any deceptive or illegal manner.

Liability of Network Service Providers

A "network service provider" (NSP) is an intermediary (Blythe, 2006). The term "intermediary" is defined as a person who acts as a service provider in respect to the delivering, receiving, preserving, or processing of electronic communications or the provision of related services (ETO, s. 2(r)), whereas a person owning, possessing, operating, managing or controlling a "public switched network" or providing "telecommunication services" is designates as an NSP (ETO, s. 2(s)). As a general rule, NSPs are immune from civil or criminal culpability for any violation of any provision of ETO by a person not under their control or direction. However, they cannot escape liability on proof of intent to facilitate, aid or abet any violation of any provision of ETO ((ETO, s. 40).

Suggestions

The following suggestions are made to improve ETO and CSPAR:

1. Regarding the criminal liability of CSPs implicated in the issuance of fraudulent certificates, the law states nothing about the operational assets of such CSPs. The confiscation of any ill-gotten gains acquired by CSPs is essential for the proper administration of justice and to deter such conduct. As an additional penalty, the ETO shall be amended to provide for the confiscation of operational assets.
2. In addressing the legitimacy and acceptance of foreign certificate suppliers, the ETO is silent. Furthermore, the concept of reciprocal recognition is not mentioned anywhere in the legislation. Reciprocal recognition of CSPs must be included as an extra requirement in the

ETO to allow international acceptance and execution of electronic documents and electronic signatures.

3. The ETO is silent on consumer protection and the right to data privacy in online contracting. Even though the measure pertaining to electronic data protection has been under contemplation since 2005, the legislature must improve the laws by incorporating consumer protection laws applicable to cyberspace.
4. Wills are excluded from the ETO. Consequently, a will must be written on paper accompanied with a handwritten signature. As other jurisdictions recognize the legal validity of electronically executed testaments (Ross, 2004), this restriction should be eliminated.
5. Since separation of judiciary from executive is a constitutional requirement in Pakistan and specialized knowledge is frequently necessary in the adjudication of E-commerce issues, Information Technology Courts should be formed as a court of first instance in place of authorized officer or committee of the CC.
6. Currently, the ETO allows public authorities to communicate with individuals through the acceptance or issuing of electronic documents. However, they have no obligation to switch to electronic format. This must be revised. Whenever practicable, it should be mandatory on government entities to accept and issue electronic documents, rather than having the option to do so voluntarily. This would increase E-government, leading to greater citizen ease, improved effectiveness, and lower costs.

Conclusion

Electronic signatures and papers are valid under ETO law. The statute employs a two-tiered approach in that it provides minimal legal recognition for several types of digital signatures while granting additional legal advantages (e.g., presumption of validity) to advanced electronic signatures with enhanced security features. Accordingly, the ETO establishes a mandatory licensing system for CSPs, stipulates exhaustive rules for adherence, and ascribes the duty of supervising their activities to the CC. In addition, the CC has promulgated the CSPAR, which specifies, inter alia, the terms and conditions, duration, fee, and procedures for evaluating petitions for “grant, renewal, suspension, or revocation of accreditation”. Overall, ETO and CSPAR provide a firm basis upon which future E-commerce and E-government can be raised. However, in order to align them with contemporary international E-commerce laws, the following amendments are suggested: (1) provide confiscation of operational assets of CSPs involved in issuing false certificates; (2) ensure that overseas CAs and certificates are acknowledged reciprocally; (3) add consumer and data protections; (4) recognise the legal validity of electronic wills; (5) create Information Technology Courts as E-commerce's first-tier courts and (6) mandate public authorities to accept and issue electronic documents.

References

Adams, C., & Lloyd, S. (1999). *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Sams Publishing.

Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S., & Kar, J. (2014). Public key infrastructure: A survey. *Journal of Information Security*, *6*(01), 31.

American Bar Association, Digital Signature Guidelines (1996).

Arslan, Z. (2015). Electronic signature and current advancements. *GSI Articletter*, 13, 103.

Basu, S., & Jones, R. (2003). E-commerce and the law: a review of India's Information Technology Act, 2000. *Contemporary South Asia*, *12*(1), 7-24.

Biddle, C. B. (1997). Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace. *San Diego L. Rev., 34*, 1225.

Blythe, S. E. (2006). A critique of India's Information Technology Act and recommendations for improvement. *Syracuse J. Int'l L. & Com., 34,* 1.

Blythe, S. E. (2009). *Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act*, a book chapter in Internet Policies and Issues, Frank Columbus, Ed., Nova Science Publishers, Inc., New York NY.

Boss, A. H. (2009). The Evolution of Commercial Law Norms: Lessons to be Learned From Electronic Commerce. *Brooklyn journal of international law, 34(3).*

Blythe, S. E. (2010). Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As A Sign of Hope for A Troubled Nation. *International Business Research,* 3(1), 151.

California Secretary of State, California Digital Signature Regulations: California Government Code Section 16.5.

Certification Service Providers' Accreditation Regulations, 2008 (Pakistan).

Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE*, 76(5), 560-577.

Electronic Transaction Act, 2002 (Pakistan).

Electronic Signature Act 1996 (Florida).

Fischer, S. F. (2001). Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. *BUJ Sci. & Tech. L., 7,* 229.

Haileyesus, I. W. (2021). An appraisal of electronic signature law of Ethiopia: further reforms for improvement. *International Journal of Public Law and Policy*, *7*(1), 49-73.

Khan, J. R. K. U. R. (2012) Cyber Laws in Pakistan

Khan, T. A.(2015) Legal Environment of E-commerce in Pakistan.

Kim, H. (2019). Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. *Computer Law & Security Review*, 35(5), 105315.

Mason, S. (2016). *Electronic signatures in law*. University of London press.

Osty, M. J., & Pulcanio, M. (1999). The Liability of Certification Authorities to Relying Third Parties, 17 J. Marshall J. Computer & Info. L. 961 (1999). *UIC John Marshall Journal of Information Technology & Privacy Law*, *17*(3), 9.

Pun, K. H., Hui, L., Chow, K. P., & Tsang, W. W. (2002). Review of the electronic transactions ordinance: can the personal identification number replace the digital signature. *Hong Kong LJ*, 32, 241.

Reed, C. (2001). Legally binding electronic documents: digital signatures and authentication. In *Int'l L.* (Vol. 35, p. 89).

Richards, R. J. (1998). The Utah digital signature act as model legislation: A critical analysis. *J. Marshall J. Computer & Info. L.,* 17, 873.

Roland, S. E. (2001). The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues? *Suffolk University Law Review 35*, 638.

Ross, C. M. (2004). Probate-Taylor v. Holt: The Tennessee Court of Appeals allows a computer generated signature to validate a testamentary will. *U. Mem. L. Rev., 35,* 603.

Satizábal, C., Forné, J., Hernández-Serrano, J., & Pegueroles, J. (2006). Building hierarchical public key infrastructures in mobile ad-hoc networks. In *Mobile Ad-hoc and Sensor Networks: Second International Conference, MSN 2006, Hong Kong, China, December 13-15, 2006. Proceedings 2* (pp. 485-496). Springer Berlin Heidelberg.

Smith, B. W., & Kiefer, K. B. (1999). Recent Developments in Electronic Authentication: The Evolving Role of the Certification Authority. *Banking LJ*, *116*, 341.

Smedinghoff, T. J. (1998). Certification Authority Liability Analysis. Available at SSRN 2602207.

Srivastava, A. (2012). *Electronic signatures for B2B contracts: evidence from Australia.* Springer Science & Business Media.

U.N. Convention on the Use of Electronic Communications in International Contracts, G.A. Res. 60/21, U.N. Doc. A/RES/60/21 (9 December 2005)

UNCITRAL Model Law on Electronic Commerce 1996, U.N. Doc. A/Res/51/162/Annex, U.N. Sales No. E.99.V.4 (1999)

UNCITRAL Model Law on Electronic Signatures 2001, U.N. Doc. A/Res/56/80, U.N. Sales No. E.02.V.8 (2002).

UNCITRAL, Report of the United Nations Commission on International Trade Law on the Work of Its Seventeenth Session, para. 135–136, U.N. Doc. A/39/17 (1984).

Utah Digital Signature Act 1995.