UCP Journal *of* Law & Legal Education
Vol. 2, Issue 1 (July - December 2023)

# Laws Governing eSignatures in Pakistan: An Overview

***Sajjad Ali****

## Abstract

*Living in a tech-oriented world, we witness that technology plays a crucial role at each stage of our lives. Within commercial spheres also, technology occupies a prominent place due to its potential, inter alia, to improve efficiency and provide security. In the same vein, electronic signatures (eSignatures) have become an ordinary part of and are being used frequently in commercial transactions. In 2002, legislation for digitization of the conduct of business and regulation of eSignatures was adopted under the title 'The Electronic Transactions Ordinance, 2002'. This law validated the use of eSignatures in Pakistan. Following doctrinal research methodology, this article examines the legislation governing eSignatures in Pakistan. It analyses the documents that can be eSigned and the documents that cannot be, followed by an in-depth evaluation of the admissibility of eSignatures and advanced eSignatures in the court and an analysis of the threshold of validity of each respectively. It, then, discusses the distinction between eSignatures and advanced eSignatures. Finally, it assesses the risks and challenges arising from reliance on eSignatures.*

**Keywords**: Law-tech, electronic signatures, advanced electronic signatures, technology,

## Introduction

Digital advancement has made a huge impact on the development of law. The present era is full of technological inventions, and innovations. The growing technological advances have also impacted the existing laws and the approach of society towards them.

The advancement of the business towards paperless workflows has led to the adoption of electronic signatures worldwide. In Pakistan, eSignatures are regulated by the Electronic



*****Judicial Law Clerk at Islamabad High Court email: advsajjadbaloch@gmail.com

Article History: Received; 20 June 2023; Received in revised form; 6 November 2023; Accepted: 20 December 2023.
Available online: 30 January 2024

Transactions Ordinance, 2002 (ETO). ETO confers legal recognition to eSignatures. It expressly provides that if any law requires that a document should be signed by the bearer then such signature would be deemed legally valid if it has been eSigned. Article 164 of the Qanun-e-Shahadat Order, 1984 (QSO) also recognizes the legal validity of eSignatures as proof of presumption to an eAgreement. Additionally, it confers recognition to eRecords as documentary evidence.

Although eSignatures have been adopted worldwide and are currently in use, nonetheless, their applicability and legal validity have remained controversial in Pakistan. This is because the majority of the people in Pakistan have not fully understood the benefits of eSignatures. Owing to various security concerns, people are afraid of relying on eSignatures and they tend to remain more attracted to the traditional paper-pen signature rather than relatively new eSignatures (Mutabazi, 2021). Therefore, legal validity and recognition accorded to eSignatures must be delved into in-depth to raise general awareness among the masses. Although the Electronic Transactions Ordinance, was enacted in Pakistan 21 years ago in 2002, this is the first research where a framework concerning the eSignatures is being evaluated in depth. Moreover, the paper also explores the distinction between eSignatures and advanced eSignatures commonly known as digital signatures. The aims of this paper are:

i) To analyse and examine the legislation governing eSignatures in Pakistan and to draw a distinction between eSignatures and advanced eSignatures or digital signatures.
ii) To make an in-depth analysis of why eSignatures should be preferred over traditional signatures.
iii) To evaluate the admissibility of eSignatures and advanced eSignatures in the court and to analyse the threshold for the validity of eSignatures and advanced eSignatures.
iv) To identify the documents that cannot be signed electronically or digitally.
v) To assess the risks and challenges arising from reliance on eSignatures.

By achieving the five-fold aims mentioned above, this research study will make a worthy contribution to the research on electronic

signatures as it adds to the global discussion on eSignatures and the distinction between eSignatures and advanced eSignatures.

## Research Methodology

In conducting this research, the Doctrinal Research Methodology is adopted. While adopting this methodology the author has conducted an in-depth and descriptive analysis of the relevant literature by identifying those specific legal rules that are relevant to the problem of the present research study.
The data includes:

a) Text of the Electronic Transactions Ordinance, 2002, and the model law on the electronic transaction of 2001, namely the United Nations Commission on International Trade Law (UNCITRAL).
b) Commentaries and literature available on the research topic, for instance, research articles, research papers, and database sources.

## Literature Review

The concept of eSignatures or digital signatures was advanced by Heyst and Chaum in 1991. According to him, the notion of a person signing on behalf of others while receiving a message through online mode will prove to be more convenient for the whole company. Moreover, since only one authorised person will have access to the signature password, therefore, eSignature cannot be used by unauthorised persons. Additionally, the administrator himself would be in a position to verify the person who used the signature.

Maria, a tech lawyer, in her article titled eSignatures-Assessing the Legality in Pakistan, 2020, has highlighted the need for the clarification of the existing legislation governing eSignatures in Pakistan. She asserts that the existing legal framework must be discussed to raise awareness among the public at large. Apart from this, another author has expressed that various security concerns relating to electronic signatures have led people to place less reliance on them despite their efficacy. A very prominent jurist namely, Miyazaki in his article titled Digitally signed document sanitising scheme based on bilinear maps (2006) claims that when

an eSignature has been put on a document, then subsequently the contents of the document cannot be changed. Thus, it helps to ensure that the contents of the document remain unaltered and there must not exist any possibility of interference with the same. Moreover, another article by Niccache et al (2008) has rightly introduced the concept of "twinning", which has made the signing of short messages possible. Furthermore, Driessen et al (2008), while discussing the security of wireless networks, states that the Wireless Network Sensor makes the use of asymmetrical cryptography impossible. Another author Wang (2005) has highlighted the need for individuals to ensure that they receive each other's signatures online to enhance security for the concerned parties.

## Legislation Governing eSignatures in Pakistan

In Pakistan, the legislation regulating electronic signatures is the Electronic Transactions Ordinance (ETO) 2002. This law was formulated and adopted in accordance with the Model Law on Electronic Signatures 2001 laid down by the United Nations Commission on International Trade Law (UNCITRAL) in order to harmonize Pakistan's legal regime with the international regime. It is pertinent to mention that Pakistan is one of the first countries in South Asia, other than China, to regulate and recognize eSignatures through an enactment.

This above-mentioned Model Law on Electronic Signatures (MLES) has the primary objective of facilitating the use of eSignatures. It enables the employment of eSignatures by providing established criteria of reliability for the comparability between eSignatures and hand-written signatures. Thus, it would not be out of context to mention that the MLES positively aids States in manifesting a contemporary, harmonised, fair, and synchronised legal regime to effectively address the legal treatment of eSignatures and give validity to their status for its worldwide reliance. The frequent and enhanced usage of electronic authentication methods as the alternative to traditional handwritten signatures and other conventional verification procedures highlighted the need for a definite legal regime in order to lessen the uncertainty regarding the legal effect and validity that may consequently arise from the use of the electronic medium of working. To effectively respond to such needs, the MLES has been enacted that is based on the fundamental

principle underlying article 7 of the UNCITRAL Model Law on Electronic Commerce which concerns the fulfilment of the signature function in an electronic working model whereby a tech-neutral approach is followed. Thus, practically the present international legislation recognizes the digital signatures based on cryptography and eSignatures based on other technologies.

## Existing Legal Framework Under ETO, 2002

### eSignatures: Definition, Advantages and Demerits

Before discussing eSignatures, it is significant to define what a signature is.

So, the term signature refers to the depiction of a mark, usually in the form of a name on a document as proof of the person's identity in authorising a document.

Section 2(1)(n) of the ETO provides a legal definition of eSignatures in the following words;

> "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".

Furthermore, Article 2(a) of the UNCITRAL also provides an internationally recognised definition of eSignatures. According to Article 2(a) the Electronic signature means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

Thus, eSignature is legally valid, binding, and secure. It can be in the form of a symbol, process, or even an image that may be affixed to the document or any short message for recognising an individual's identity. It indicates the consent of the signer to be bound by the terms of the documents wherein he has put his signature. eSignatures are used in those cases when the verification of the documents is necessary.

Some of the benefits or advantages of eSignatures include convenience, time-saving, and cost-effectiveness. eSignatures are

more convenient and easier to use because they allow documents to be signed virtually or remotely from any far location. Therefore, it proves highly advantageous for individuals and companies indulged in multi-national businesses because the employees or the clients can easily eSign the documents without ensuring their physical presence. Secondly, they are more time-saving because eSignatures can be used instantly to sign documents. Thus, it saves the time that gets wasted in mailing, scanning, or faxing documents that have been signed with traditional handwritten signatures. Finally, these signatures are highly cost-effective. It helps to save the considerable amount of money that needs to be paid for the paper, postage, ink, or any other ancillary expenses. Moreover, eSignatures can be encrypted thus making them more secure, and authentic, and thereby the risk of unauthorised access can be reduced.

Despite having advantages, there are some demerits of eSignatures. For instance, these are prone to technical issues, such as system failures. Furthermore, eSignatures are excessively dependent on technology like reliable internet connections and computers. This could prove somewhat problematic in those places where there is limited technological infrastructure.

**Advanced eSignatures- Definition, Advantages and Demerits**

Section 2(1)(e) of the ETO provides a legal definition of advanced signatures in the following words;

'Advanced electronic signature' means an electronic signature that 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 the authenticity and integrity of an electronic document.

There exists a difference between eSignatures and advanced eSignatures. According to section 2(1)(e) of the ETO, an advanced eSignature is also a subcategory of eSignatures but it has additional features. It is an eSignature that is unique to the person who is signing it and it has the capability of identifying the person who has signed it (Jena, 2022). In this additional user authentication step, the person who would be signing will be required to produce and use a valid document in order to confirm their identity and a specific unique access code after the procedure of signing. Advanced eSignatures also make it mandatory that a digital certificate must be generated and affixed to the document as part and parcel of the transaction (Jena, 2022).

Advanced eSignatures are also commonly known as Digital Signatures. It refers to a more secure and authentic signature that works with eSignature and relies on the Public Key Infrastructure (PKI) (Jena, 2022). The PKI refers to the coding and encryption standards. It can be envisioned as an electronic fingerprint that helps to authenticate a person's identity, who has signed the document digitally (Jena, 2022). Once, a document has been signed electronically by the parties, the same is secured and sealed with the help of PKI. This seal helps in the verification of eSignature and indicates the non-tempering of the document (Jena, 2022). PKI is a standard technology that provides a high level of security and protects against fraud. Whenever companies intend to secure a document, they make use of a digital signature. In every state, including Pakistan, there has been established a trusted certificate authority that performs the essential duty of the validation of digital signatures. The certification by this trusted certificate authority thus authenticates the digital signature consequently making it more secure and less vulnerable to fraud, hacking, or cyber-security risks. Owing to this reason, a digital signature is given more preference over eSignatures. Moreover, digital signatures utilize advanced cryptographic procedures to make them more secure which in turn reduces the risk of getting accessed by unauthorised persons. (Jena, 2022). It is pertinent to mention that digital signatures provide a non-repudiation procedure thereby a person who has once signed the document cannot deny his or her signatures. In addition to this, another advantage of digital signature is time stamping. By time stamping, it is meant that digital signatures include a time stamp that provides a record of the date and time when the document was

signed (Mutabazi, 2021). Furthermore, it also shows the time of any further amendment or alteration that might have been made in the documents after digital signatures (Mutabazi, 2021).

Everything has its merits and demerits. This applies equally well to digital signatures too. Despite having various benefits and advantages, digital signatures, too, have some demerits. The first disadvantage relates to its highly compact and complex nature. Digital signatures are usually more complex to create and utilize than traditional signatures (Jena, 2022). They require a piece of specialised knowledge and software and cannot be easily created or understood by the individuals lacking requisite technical knowledge and specialisation. They are too expensive and can incur more hefty costs owing to the need for the requisite hardware and software.

**eSignatures and Digital Signatures: Difference**

Although, the expressions digital signatures and eSignatures are used interchangeably, however, there exists a significant difference between both of them. This distinction was recognised by the European Council. The European Council on Technology issued a directive in the year 1999 whereby it distinguished between eSignatures and advanced eSignatures/digital signatures (EU Directive, 1999). It provided that digital signatures are equally admissible in legal proceedings and have a comparatively higher security level than eSignatures (EU Directive, 1999).

The primary difference between them is that in the case of eSignatures there is no requirement to follow a particular technological process (Jena, 2022). Meanwhile, when it comes to digital signatures, they require a specific technological process to be followed. Digital signatures are more reliable and cannot be easily tampered with because a digital signature has a higher degree of authenticity integrity and legal value as it is issued by an authority that is called the certification service provider (Jena, 2022).

The major points of distinction between an eSignature and digital signatures (eMudhra,2021) have been outlined below in tabular form.

Table 1: Distinction between an eSignature and digital signatures

| **eSignatures** | **Digital Signatures** |
|---|---|
| The expression eSignature is a broader term than digital signatures. An eSignature is not necessarily deemed to be a digital signature. | A digital signature is a sub-category of eSignatures. Thus, all digital signatures are eSignatures but not all eSignatures are digital signatures. |
| eSignature can be in the form of an image, process, or even a symbol that might be attached to the document for recognition of the identity of the person and to establish that he has consented to it. | On the other hand, a digital signature can be envisioned as an electronic fingerprint that encodes and identifies an individual's identity. |
| An eSignature is less secure when compared with digital signatures. Since it lacks the secure coding method as is found in digital signatures. | On the contrary, a digital signature is more secure reliable, and authentic owing to the presence of the coding procedure that is followed for the authentication and its reliability. |
| Owing to security concerns eSignatures are not as widely accepted globally as digital signatures. | Digital signatures have been recognised and accepted worldwide as they fully meet international standards for security. |
| Due to their less secure nature, eSignatures can be easily altered, tampered with, or copied. | The digital signatures cannot be tampered with, altered, or copied because of the advanced security procedures. |
| eSignatures can be used for the purpose of verifying a document. | Meanwhile, it is primarily utilised for securing a document. |
| The validation and authorization of eSignatures are not conducted by the trusted certificate authorities | However, in the case of digital signatures, a trusted certificate provider and trust service provider perform validation. |

| | |
|---|---|
| or any of the trust service providers. | |
| No coding mechanism is utilised in eSignatures. | While in the digital signature secure encryption standards are incorporated. |
| eSignatures cannot be verified. | While a digital signature can be verified. |
| The widely used types of eSignatures include Verbal, electronic ticks, or scanned signatures, etc. | The common types of digital signatures include Microsoft, Adobe, and DocuSign. |
| eSignatures are widely employed in contracts and agreements. | Since a digital signature makes use of a digital certificate to verify the person's identity, thus, it is a better and more secure tool for sensitive data such as financial records. |

Thus, the security, authenticity, and integrity of electronic documents are ensured by the eSigning procedure. Digital signatures provide a more secure alternative to ensuring the authenticity of documents. Additionally, they have proven to be more convenient and efficacious. The significance of digital signatures continues to increase as we move towards a tech-oriented world.

**The Electronic Certification and Accreditation Council**

The primary purpose of the signatures is to ensure authenticity and credibility thus putting the signatures signifies trust and reliability. eSignatures are, however, susceptible and prone to misuse and may raise various security concerns, specifically in the present era (Bajwa, 2023). Owing to security concerns a need for the establishment of the certification body arose. This resulted in the formation of the Electronic Certification and Accreditation Council (ECAC). It was established for the purpose of authentication and certification of eSignatures. It also provides a framework for certifying authorities throughout the country.

The ECAC has been established in Pakistan according to Section 18 of the ETO. It is an autonomous body that is working under the Ministry of Information Technology and Telecommunication. Being, a regulatory body, ECAC has the authority to enforce and regulate electronic transactions in the private as well as public sectors as provided under section 18 of ETO.

The ETO also empowers the ECAC to regulate the accredited certifying service providers (CSPs) and Certifying Authorities (CAs). The expression accredited certifying service providers has been defined under section 2(1)(c) of the ETO and it means a Certification service accredited under the ETO to issue certificates for the use of cryptography services. Whereas CAs are authorised to issue digital signature certificates for electronic authentication, ECAC has the authority to audit and regulate the CSPs under Section 4 of Accredited Certification Service Provider's Audit Regulations 2008, and it can audit and regulate the CAs pursuant to the Certification Service Providers' Accreditation Regulations 2008.

Furthermore, pursuant to Section 21(2)(d) of the ETO, the ECAC is duty-bound to establish and manage the repository of the certificates that shall contain all digital certificates issued by the CAs. The digital signature certificate verifies the identity of the signature and the person electronically. Moreover, ECAC plays a significant and central role in ensuring compliance with the recommendations in the Guidance on Digital Identity that was issued by the Financial Action Task Force in March 2020 (Financial Action Task Force, 2020).

Section 21 of the ETO lays down the functions to be performed by the ECAC. It, firstly, provides that the Council shall perform such functions as are prescribed in the ETO, and additionally, it is duty-bound to perform other functions too as discussed below.

According to section 21(2), ECAC is duty-bound to grant and renew accreditation certificates to the service providers as defined above. Secondly, it has the obligation to monitor whether certificate service providers are duly acting in compliance with the terms of accreditation. In case ECAC finds that service providers have failed to comply with the prescribed terms then it has the right to revoke or suspend the accreditation granted to them while

outlining the reasons therein. Thirdly, it is mandated to ensure the compliance of the certification service providers with the relevant provisions of the ETO. Fourthly, it has to establish and manage the repository. Fifthly, it is required to conduct research concerning cryptography and may also seek the opinion of the general public in this regard. Finally, it is mandated to encourage and ensure uniformity in standards and practices throughout the country.

## Why eSignatures Should be Preferred over Traditional Signatures?

We may find a controversy in Pakistan; whether eSignatures should be used or conventional ink-paper signatures be utilised? This paper proposes that electronic signatures are more secure and convenient than conventional pen and paper signatures. The traditional pen-paper signatures are outdated and inconvenient in modern times. Before stepping into the digital era, paper signatures were widely used and regarded as the most secure method of transactions and signing documents. It is believed that paper signatures are more secure because digital signatures are more vulnerable to cyber-attacks. Traditional paper signatures are not secure and convenient because there are various risks associated with them too. For instance, paper copies are prone to destruction owing to natural disasters like fire, water, or even at home they could get damaged due to spilling of any liquid. This risk could be effectively tackled by eSignatures as they are not subject to destruction due to the aforementioned causes. eSignatures can be effectively utilised to gain access to cyber security measures that are useful to protect the information from cyber-attacks as well as other potential breaches of security. Furthermore, eSignatures can help in the eradication of bulky file cabinets thereby making the work easier and less stressful. It plays a crucial role in the protection and preservation of important documents and greatly reduces the risk of losing significant information. Thus, eSignatures are more secure and efficacious as compared to paper signatures (Sen, 2022). Therefore, eSignatures are a better alternative to traditional pen-paper signatures. They fulfil the legal requirement and also provide written evidence of the intention of the parties to be bound by the terms of the agreements.

## Legal Validity and Recognition of eSignatures and Advanced eSignatures

Under the ETO, 2002, eSignatures are considered to be valid and legally binding in Pakistan, thereby making them legally admissible in the courts of law. ETO grants legal recognition and validity to eSignatures and provides that they shall be presumed to be legally admissible unless rebutted. Section 7 of the ETO expressly provides;

> The requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signature are applied.

Moreover, section 8 of the ETO answers the question of how eSignatures can be proved. It states;

> 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.

Thus, according to Sections 7 and 8 of the ETO, eSignatures and advanced eSignatures are legally valid and recognised in the law. Sections 7 and 8 of the ETO are based on the Model Law on Electronic Signatures in compliance with the UNCITRAL.

Since, Pakistan is also a signatory to the UNCITRAL therefore, the case laws of the other states based on UNCITRAL may be considered persuasive in Pakistan's legal framework too. The reference here may be made to the renowned case of the *Golden Ocean Group Ltd vs Mining Industries Pvt. Limited* before the England and Wales Court of Appeal wherein the court recognised the informal email signatures to be valid and legally binding (2012 EWCA Civ 265). This case involved a contract of guarantee wherein the relevant statute required that for being legally enforceable it must be signed by or on behalf of the person giving the guarantee. It formed a series of emails. The court ruled that since it formed part of emails therefore it would suffice as an eSignature and no formal signature was necessary (2012 EWCA Civ 265).

Moreover, reference may also be made to a landmark judgment by the UK jurisdiction rendered by the England and Wales High Court of Justice. The case titled *Neocleous v Rees*, 2019 EWHC 2462 (Ch) considered the question of whether an eSignature is enforceable in the case of contracts. The parties in this case had

agreed to execute a proposed sale of land. They negotiated the terms and conditions of the sale through a series of emails between their respective counsels. The terms of the contract were agreed to be confirmed through emails, however, no separate documentary contract was finalised or executed in this regard.

The defendant claimed that since no written/ documentary contract was formulated, therefore, it couldn't be deemed a valid contract. On the contrary, the claimant contended that the respective emails regarding the terms of the settlement amounted to a contract and thereby he sought its specific performance. The High Court of Justice of England and Wales ruled that the email signature was sufficient to meet the legal requirement of the law of contract and the claimant was entitled to specific performance of that contract.

The court further observed the following in relation to eSignatures:

Firstly, the word 'signature' no longer requires a handwritten signature as it includes the signature that is usually provided at the footer of the email, which outlines the sender's name, contact details, occupation, and relevant role.

Secondly, it has been observed that if there is an auto-generated footer in the email then it does not necessarily indicate a lack of intention on the part of the person/sender of the email. Because the measures taken to set up a rule that applies a signature at the footer of emails indicates a conscious decision on the part of the sender. Thus, it could be validly deemed that the sender of the email was fully cognizant of the fact that his or her name was being affixed to the footer of the email and the recipient needs not to question that as the recipient lacked the requisite knowledge that signature in the footer was auto-added or was manually put thereon (*Neocleous v Rees*, 2019 EWHC 2462 (Ch)).

## Thresholds for Placing Reliance on eSignatures and Advanced eSignatures

Although, ETO has granted the legal validity, recognition, and admissibility to eSignatures, that however, is not absolute. ETO has specified the limitations and provided the threshold which needs to be reached before placing reliance on eSignatures.

## Threshold for eSignatures

The following thresholds have been specified for eSignatures under ETO:

Firstly, under section 2, if a document is alleged to be eSigned or to have been generated digitally wholly or in part, or by use of an information system and if such allegation is denied, then the security procedure that was applied to the signature or document needs to be proved for the purpose of satisfying the evidentiary requirement established under the Qanun-e-Shahadat Order, 1984 (Article 78, QSO, 1984).

Secondly, Section 7 of the ETO mandates that the requirement under any law for the affixation of signatures shall be deemed to be duly fulfilled if eSignatures or advanced eSignatures have been placed.

Thirdly, section 8 of the ETO provides that an eSignature should be proved to verify the identity of the person who has executed it.

## Threshold for Advanced eSignatures

The following thresholds have been specified for the advanced eSignatures under ETO:

Firstly, under Section 7 of the ETO, it is mandated that the requirement under any law for the affixation of signatures shall be deemed to be duly fulfilled if eSignatures or advanced eSignatures have been placed.

Secondly, in any proceedings concerning an advanced eSignature, ETO recognises the following presumptions, unless it is rebutted by the evidence, an eDocument wherein any advanced eSignature has been affixed is deemed to be authentic and has integrity. Moreover, as per section 7 of ETO, the advanced eSignature is the signature of the individual to whom it corresponds, and the advanced eSignature has been placed by that individual with the intention of and for the purpose of signing the document and that such document has not been tampered with or altered since then.

## Documents for which eSignatures are not valid in Pakistan

The admissibility and the legal validity of eSignatures are not absolute as there are certain limitations concerning specific documents. Certain categories of transactions have been excluded under ETO.

Section 31 of ETO bars the applicability of provisions of the ordinance to documents created by certain laws. It provides that the ordinance shall not apply to the Negotiable Instruments as defined under section 13 of the Negotiable Instruments Act, 1881. Thus, eSignatures or advanced eSignatures are not valid or enforceable with respect to the negotiable instruments. Secondly, it does not apply to the Power of Attorneys as defined in the Power of Attorney Act, 1881. Hence, a power of attorney cannot be digitally signed, and if signed would not have any legal validity. Thirdly, its applicability is barred in relation to the trust as defined in the Trust Act, 1882 as per Section 31 of ETO. Fourthly, it shall not apply to the wills or any other testamentary documents. Finally, it doesn't apply to contracts for sale or conveyance of immovable property or any interest therein as per Section 31 of the ETO.

These documents require conventional handwritten signatures that are currently in use, thus, they need to be manually authenticated because eSignatures or digital signatures do not apply to these documents.

## Risks and Challenges Associated with eSignatures

Despite the wide acceptance and usage of eSignatures, various security concerns have been raised since it is a relatively new technology. Data integrity is the main purpose of digital signatures. They make it possible for users to ensure the safety and authenticity of the data that they are dealing with (Matran, 2019). Thus, its primary goal is to ensure that any party to an electronic communication can be held liable for accepting the authenticity of the signature they apply on any document (Matran, 2019).

However, digital signatures are prone to various security vulnerabilities. One of the strategies used by cyber threat individuals includes the theft of private trusted keys to sign fake, forged, and fabricated documents to make those forged documents appear original and trustworthy. The security issues range from simple data

theft by virtue of network infiltration to systematic, thought-out, and planned cyber-attacks (Matran, 2019).

Furthermore, another risk relates to the exploitation of the vulnerabilities that exist during the execution of eSignatures. This is because, at the time of execution of eSignatures or digital certificates, the system algorithm overlooks the storage size of the header (Matran, 2019). That in turn provides extra space for the developers to attach links to update and add new content without requiring any signature again (Matran, 2019). Furthermore, this header storage data can also be manoeuvred by hackers to add additional data that might prove harmful to the user. Thus, software algorithms have the potential to cause serious risks to data privacy and integrity.

In order to highlight the risks arising from the electronic systems reference may be made to the Verisign attack incident. (Zetter, 2012).

In this case, an internet company namely Verisign, experienced a serious attack that was caused by the signature fabrication malware known as Troj/Browser Helper Object-QP. This malware remained hidden under the Flash player extension from Microsoft. This potentially dangerous malware was employed for the installation of a fake "VeriSign Class 3 Code Signing 2009 CA" root certificate which allowed the malware to be kept away from being declared as unauthentic and not verified. This malware poses serious and various types of cyber threats, for instance, phishing and unauthorised data collection through installation of the undesirable and harmful extensions (Zetter, 2012). The attack was highly complex and well-planned by the hackers resulting in serious damage to the systems (Zetter, 2012).

Challenges and risks associated with eSignatures include forgery. Forgery or theft of the identity is one of the serious challenges arising from placing reliance on eSignatures. This risk, however, can be greatly reduced if eSignatures are secured with password encryption and two-factor authentication. In addition to forgery, there is also another risk of fraud. By fraud, it means that a person having gained authorised access may alter a digitally signed document (Zetter, 2012). This risk is not only confined or limited to eSignatures or digital signatures but it equally causes problems in the case of pen paper signatures.

Courts in various jurisdictions have also highlighted the risks associated with the electronic mode of communication. In 2016 the Supreme Court of New South Wales (NSWCA) in the case of *Williams Group Australia Pvt Ltd v Crocker* (2016) observed that though widely relied upon, eSignatures are prone to many risks. In this case a company creditor namely, Williams was not able to enforce a guarantee signed with eSignature wherein the amount of debt was approximately $900,000. The Court held that whenever an eSignature is employed to execute an agreement, the party adopting the signature should take into account the risk of forgery or improper use by taking certain measures to assess that the signature has been put genuinely with the consent of the individual concerned (*Williams Group Australia Pvt Ltd v Crocker* (2016), para 34).

Furthermore, owing to the various security risks and challenges, the courts are currently highly reluctant to rule that there has been an acknowledged mentor for the ratification of an unauthorised use of an eSignature until clear and substantial proof is produced to show that the person who has signed the document electronically has done so with the consent and with a full understanding of the consequences of eSignature (Douglas Cheveralls Lawyers, 2018).

## Conclusion and Recommendations

Living in a tech-oriented world, it has become the need of the time that every citizen must be able to properly understand the legal procedure and law relating to electronic transactions.

The ETO expressly defines and provides an in-depth elaboration of eSignatures. However, still, there exists a need for the development of a law regulating the system of authentications to make it simple and uncomplicated for the general public. Moreover, owing to the security concerns, it is recommended to adopt those methods that are less vulnerable to fraud and tampering and in case of any risk, the same should be avoided. Furthermore, to halt the various security-related risks, it is recommended that documents should be secured with password encryption and two-factor authentication, wherever applicable. Securing the documents by these methods can play pivotal role in reducing forgery, fraud, and other cyber-security concerns. Given that eSignatures are binding and legally valid and recognised by the law on equal footing as hand

signatures, therefore, it becomes essential for citizens to use them with proper caution and understanding. In the present era, professionals are using eSignatures regularly in the day to day affairs, therefore, it is significant to have an efficient authority to tackle the existing loopholes in the laws and regulations. The vision of digital Pakistan can be made effective and significant by providing a better mechanism of authentication and frequent use of technology (Bhatia, 2021). In the current times, where the online medium has become a need of time for every person, there is a need for proper guidelines regarding the usage of eSignatures. eSignatures have the potential to make a transitional shift towards digitisation.

## References

Accredited Certification Service Provider's Audit Regulations 2008. Section 4. Accessible at https://ecac.gov.pk/wp-content/uploads/2020/09/ECAC-Service-Provider-Audit-Regulations-2008.pdf

Bajwa, S.S. (2023). Legality and Validity of eSignatures in Pakistan. *Courting the Law*. Accessible at <https://courtingthelaw.com/2023/02/13/faqs/how-to-guide/legality-and-validity-of-eSignatures-in-pakistan/#_ftnref3>

Bhatia, A & Katiyar, S. (2021). ESignatures- the legal validity, *Blog Ipleaders,* available at: https://blog.ipleaders.in/eSignatures-the-legal-validity/

Certification Service Providers' Accreditation Regulations 2008. Section 8. Accessible at https://ecac.gov.pk/wp-content/uploads/2020/09/The-Certification-Service-Providers-Accreditation-Regulations-2008-updated.pdf

Chaum, D., & Van Heyst, E. (1991). *Group signatures. In Advances in Cryptology*—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10 (pp. 257-265). Springer Berlin Heidelberg.

Chen, L & Paterson, G. (2004). *Hewlett Holloway laboratories, Bristol UK, 'Concurrent Signatures'.* The University of London, 287-305.

Diffie, W, Hellman, M (1976). 'New Directions in Cryptography': Information Theory. *Institute of Electrical and Electronics Engineering Transactions*, *22*, 644-654, p. 650.

Douglas Cheveralls Lawyers. (2018). Electronic Signatures: Benefits, Risks, and a Cautionary Tale. Available at; https://www.dclawyers.com.au/articles/electronic-signatures-benefits-risks

Driessen, B, Poschmann, A and Paar, C. (2008). *Comparison of innovative Signature Algorithms for WSN*. WiSec '08: Proceedings of the first ACM conference on Wireless network security, Alexandria, Virginia, USA, New York, NY, USA, ACM, 30-35, p. 33.

eMudhra.(2021). What is the difference between a Digital Signature and an Electronic Signature? Available online at; https:// emudhradigital.com/kc/what-is-the-difference-between-a-digital-signature-and-an-electronic-signature# :~:text=An%20electronic%20signature%20is%20simply, digital%20signature%20secures%20a%20document.

Financial Action Task Force (2020), *Guidance on Digital Identity, FATF*, Paris. Para.90 Accessible at <https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf>

*Golden Ocean Group Ltd vs Mining Industries Pvt. Limited* (2012 EWCA Civ 265), 45.

Jena, S. (2022). Difference between Electronic Signature and Digital Signature. GeeksforGeeks. Available at; https://www.geeksforgeeks.org/difference-between-electronic-signature-and-digital-signature/

Matran, B. (2019). Digital Signatures are the Cybersecurity Vulnerability You Need to Stop Ignoring. CybelAngel.

available at;https://cybelangel.com/digital-signatures-are-the-cybersecurity-vulnerability-you-need-to-stop-ignoring/

Miyazaki, K. Hanaoka, G & Imai, H. (2006). *Digitally signed document sanitizing scheme based on bilinear maps.* ASIACCS '06: Proceedings of the ACM Symposium on Information, computer and Communications Security, Taipei, Taiwan, New York, NY, USA, 343 – 354.

Naccache, D, Pointcheval, D and Stern, J. (2001). *Twin signatures: an alternative to the hash-and-sign paradigm.* CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security, press, 20-27.

National Assembly of Pakistan, Electronic Transactions Ordinance 2002. Accessible at<http://www.pakistanlaw.com/eto.pdf> section 18, 31.

*Neocleous vs Rees,* (2019) EWHC 2462 (Ch) para 20.

Qanun-e-Shahadat Order, 1984 (Presidential Order No.10 of 1984). Accessible at <https://punjabpolice.gov.pk /system/files/ qanun-e-shahadat-order-1984.pdf>

Rivest, R, Shamir, A et al, (2006) How to Leak a Secret: Theory and Applications of Ring Signatures. *Theoretical Computer Science.*164-186.

Rivest, R,L, Shamir, A and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*. *21*(2), 120-126.

Sen, A. (2022). Security in eSignatures: The way forward in the world of Cyber-security. Certainly. available at; https://www.certinal.com/blog/eSignatures/security-in-eSignatures-the-wayforward-in-the-world-of-cybersecurity.html

Subramanya, S.R, and Yi, B.K. (2006). Digital Signatures. *Institute of Electrical and Electronics Engineering Transactions*, *25*(2), 5-8.

*United Nations Commission on International Trade Law, Model Law on Electronic Signatures with Guide to Enactment 2001*, United Nations Publication Sales No. E.02.V.8, ISBN 92-1-133653-8. Para.19. Accessible at < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf >

Wang, G. (2005). *An abuse-free fair contract signing protocol based on the RSA, signature.* Proceedings of the 14th International Conference on World Wide Web, Chiba, Japan, ACM, 412-421.

*Williams Group Australia Ptv Ltd v Crocker* (2016) NSWCA 265 paras, 30, 42,58.

Zetter, K. (2012). VeriSign Hit by Hackers in 2010. Wired. Available online at; https://www.wired.com/2012/02/verisign-hacked-in-2010/