International Journal of Academic Research [**ISSN**: 2075-4124]
Vol. 4. Issue 4. & pp.216-238 , 2016

The Impact of Electronic Signatures on Internal Control Systems

Dr. Indu Niranjan Dean GMBA Programme

Dr. A.Seetharaman Dean Academic Affairs

Prof. Veena Jadhav Assistant Dean EMBA Programme

Prof. Arindam Banerjee Director Global Immersion
S P Jain School of Global Management
Dubai-Mumbai-Singapore-Dubai

Abstract

Signatures are used in many critical business processes; electronic signatures are becoming popular in the Internet business environment especially after many countries have passed digital signature laws giving electronic signatures the same legal validity as handwritten signature. Contracts, legal documentation, and many other business processes require a series of exchanges using electronic communication such as e-mail before final sign off. The recent development in the Internet, Internet technologies, and electronic signatures technologies has altered and enable new ways in which organizations manage, transmit, and archive information. People need to feel confidence that the message received came from trusted individuals or companies, likewise when the message is transmitted, the content is not being altered during the transit and reach the person or company who he or company is he or it claimed to be. Electronic signatures help to create trust and confidence in paperless environment. This paper examines the legal implications and distinctions between different types of electronic signatures, the underpin technologies, their applications in business processes, and implications to internal control systems. A Risk Management Framework is proposed for managing security and control using electronic signatures. Not all electronic signatures are created equal. Some are more secured then the others but cost more and complex to implement. The study also examines the cost in implementing electronic signatures and the risks involved. A cost-benefit analysis needs to be done before deciding the type of electronic signature technology to be deployed It is inevitable that things will still go wrong even with the most secured electronic signatures, it is important to have an effective internal control system to complement the security and controls facilitated by electronic signatures.

1.0 Introduction

Until recently, business transactions are conducted over a known or closed domain where parties involved in the transaction are known to each other and often involved face-to-face interaction. Today, it is more economical and efficient to do business electronically especially with the growth of the Internet which has revolutionized the world by emerging as a powerful conduit for doing business globally. Chang, I. C (2007) observed that IT started form geographic commerce and moved towards electronic commerce and made the electronic signature more and more important. Accountants and internal auditors must have the skills to understand the technology underpin the electronic signatures to strengthen internal control and risk management. Many documents were controlled by providing a static RSA digital signature over selected records, which aims to prevent malpractices and other crooks. Bond, M et el. (2014)

To conduct business in a reliable, trustworthy and confidence paperless environment, the message or document transmitted must satisfy the principles of confidentiality, authentication, integrity, and non-repudiation (Marilyn Greenstein, 2000). Confidentiality refers to the unavailability of a message to non-authorized readers. On the Internet, it involves making the information unreadable by any person, usually through some forms of encryption like public key cryptography or transmitted via a secured connection like virtual private network (VPN). Authentication refers to the assurance and confidence that the person whom you are corresponding with over the other side is who he claims to be i.e. the message received really came from who the sender claims to be. In Internet application, authentication involves showing something only you have (e.g. token) or something only you know (e.g. Password, PIN number) or something only you posses (e.g. fingerprints or signature). The most common measures used in authentication are tokens, digital signatures, biometric devices, passwords, smart cards, and digital certificates. Integrity refers to the confidence that the contents of the message received are exactly the same as the contents of the message sent by the sender i.e. the message passed between two corresponding parties have not been tempered with intentionally or unintentionally by anyone. This is usually done by calculating and verifying a hash total of the message by the sender and receiver. Many countries have enacted laws and legislations to put electronic signature or digital signature on par with handwritten consent.. However, there are still many questions left unanswered on the overall enforceability of electronic contracts. There are also issues of jurisdiction and conflicts of laws since Internet by its nature are borderless and laws are territorial.

Additionally, digital signature facilitates in determining customer presence based on mobile device’s communication (Grigg, Starbuck, Hanson, Jones, Dent Munson & Bryant 2016). The rising concern over online fraud and new legislation that permits for the use of electronic signatures requires organizations to strengthen their internal control systems and building the authentication processes. The primary objectives for internal control systems are to safeguard the company’s assets, ensure the reliability of financial information, and compliance with established laws and regulations. An organization must balance between cost of implementing an internal control system and the benefits that can be derived. Chou, E. Y. (2015) indicates that while eSignatures are prevalent worldwide due to their convenience, people's perception of symbolical equivalence of handwritten and eSignature is not extensively researched topic. This study highlights the negativity associated with eSignatures due to weaker sense of social presence and involvement, regardless of various types of signatures and comfort with technology.

1.1 Research Problem and need for this research.

Replacement of traditional handwritten signature with electronic signature for approval or signing of agreement has long been touted as the next emerging technology of doing business and improving operational efficiency in a paperless environment. The transactions on digital signature are on increase. The digitally signed documents include contracts, messages via cryptographic protocol or even countless emails play a dominant role in finalizing monetary transactions running into millions. The impact of electronic signature to internal controls cannot be underestimated. In moving to a paperless environment, you introduce risk. Electronic signature has added a new dimension to risk management and internal controls. Despite many countries had enacted laws and legislations to legalize the electronic signature as equivalent to handwritten signature; however technical and cultural land mines await.

Three major problems identified in this research are:

a. Lack of framework to guide company in managing and mitigation the risks of implementing electronic signature in paperless environment;
b. The cost associated with electronic signature implementation; and
c. There is a need for an internal control system to complement the use of electronic signature

1.2 Objectives of the Research

The objectives of this research are:-

- To critically review the current legislations on electronic signatures;
- To critically review the technologies underlying the electronic signatures and digital signatures;
- To critically review the need to have an effective internal control system and the impact of emerging technologies like electronic signatures and signatures to internal controls;
- To critically review the risks associated with electronic signatures;
- To propose a Risk Management Framework for electronic signature;
- To critically the review the costs of implementing the electronic signature as a way to mitigate the risk of doing business in a paperless environment;
- To examine how internal control system can complement the implementation of electronic signatures

1.3 Scope of the Study

There are many reasons why an enterprise deploy electronic signatures like conducting on-line transaction, accessing to a network or PC or security area, accessing and verifying medical records or other personal information, security identification, retail purchasing, government and military applications, etc. This research focuses on the impact of electronic signature on internal controls from the accountant and internal audit points of view. It is not the intention of this study to focus on the technical details of different technologies used to implement the electronic signature. The study also confined basically to the application of electronic signatures in a paperless environment using Internet.

2.0 Survey of Literature

Using an electronic signature to replace a handwritten signature has long been touted as the technology will create trust and confidence in a paperless environment. This section is a review on electronic signatures based on literatures taken from various journals, text books, white papers, and Internet web sites.

2.1 Signatures and the Law

Christopher Kuner and Anja Miedbordt (1999) argue that the differences in the definition of “written signature” have great influence in the national and international policies on electronic authentication using US and Germany as references. US law is gradually reducing the scope of handwritten signature requirements by placing greatest emphasis on the intent of the parties. In contrast, German Digital Signature Law does not deal with the legal status of electronic signature but requires a high-security technical standard because of the stringent requirements for pen-on-paper signatures. From these two examples, it is not surprising that different countries frequently have quite different concepts in mind when they talk about electronic signature

Robins, Kaplan, Miller & Ciresi (2000) provide frequently asked questions on Electronic Signatures in Global and National Commerce Act (ESIGN) signed by President Clinton on June 30, 2000 and went into effect on October 1, 2000. ESIGN defines electronic signatures as "an electronic sound, or process attached to or logically associated with a contract or other record and executed or adopted by with the intent to sign the record". The ESIGN Act is a technology neutral legislation because it does not favor any particular security technology or media. According to ESIGN, electronic signature can come in many forms, including PIN numbers, passwords, or even clicking an icon. However, ESIGN does contain exceptions on the use of electronic signatures and records in some areas. It looks like it is up to the parties to the transaction to determine the form of electronic signature. In this connection, the paper by Schroers, J et al.(2015 provides an overview of development of eSignature in Belgium and German through comparing the e-signature provisions with the regulations, thereby providing the requirements of qualified electronic signatures and its application using a questionnaire format.

Daniel Uhlfelder (2000**)** provides an introduction to the Electronic Signature in Global and National Commerce Act (ESIGN), which validating the use of electronic records and electronic signatures. Digital Signature Bill (1997) defines digital signature as a public key which can accurately determine a) whether the transformation was created using the private key that corresponds to the signer's public key; and b) whether the message has been altered since the transformation was made. The Act in essence allows digital signature among others: 1) to function on electronic documents the same way as traditional handwritten signature; 2) applies to e-mail, Internet transactions, smart cards, etc; 3) allows for secured transmission of sensitive documents on the Internet.

Rath et el.(2015) observed that the increase in Foreign Direct Investments in several sectors such as services, logistics, telecom in China and its subsequent entry into World Trade Organization resulted in several reforms in regulation related to e-commerce and introduction of the 'E-signature Law'. The law grants e-signatures the same effect as handwritten signatures. However, the process of developing new laws has become very complex, causing uncertainties and likely to lead to reduced confidence in ICT and logistics industry.

Todd Hartman (2001) provides an overview of the US state and federal laws governing the need for and effect of electronic signatures. Electronic signatures and digital signatures are two different concepts that are often confused by many. Digital signature generally refers to the specific technological process of authenticating a document and a separate person agreeing to the document through the use of a public key encryption system. Electronic signature refers to any electronic mark, process or record that meets the legal requirements for verifying a document and a signatory. The author correctly pointed out the confusion between electronic signature and digital signature and it can be accepted that digital signature is really one form of electronic signature. However, different business models and environments will require different types of electronic signature for practical and commercial reasons even though electronic signature like password or pin number is considered to be a weak authentication approach but this method of authentication has been used for years in ATM card or Shell's Petrol Fleet card.

Rebecca A. Askey (2004) observed that the implementation of electronic signature may offer no greater security than a password. There is no way of verifying whether a document has been altered since the time it was signed, i.e. electronic signature does not provide any kind of signer or document authentication. Digital signatures are a specific type of electronic signature. A digital signature offers both signer and documentation authentication. The process of creating a digital signature and verifying it give the same effect as handwritten signature in terms of signer authentication, message authentication, non-repudiation, and integrity required for many legal purposes. The ability to attest the content of a message and identify of the signer make digital signature technology more superior then handwritten signature. The author provides a distinction between electronic signatures and digital signatures and argues that digital signature is more secured compared to electronic signature. However, new technology has also developed to implement electronic signature like biometrics or smart-cards to provide greater level of security especially the combination of biometric and smart-card technology. Fairchild, A. (2012) has stated that Belgium, which is considered to be on the forefront of adoption of e-ID cards, the mandatory usage of e-ID card started with citizens in 2004 and has been subsequently extended to non-Belgians and children under 12 years age. The evolution of e-ID cards and greater adoption of e-ID cards by Governments is initiating the discussion about issues pertaining to data linkage and data privacy.

2.2 Business Applications of Electronic Signatures

Today, digital signature is an integral means of implementing of cloud storage security (Rao & Yadav, 2016). Digital signature, coupled with iris features in cloud ensures its safety and security (Abbdal, Kadhim, Abduljabbar, Hussien, Yassin, Hussain, & Waley 2016). George V. Hulme (2000) believes that the ESIGN Act should make it cheaper, faster, and easier to conduct electronic business over Internet. E-signature or electronic signature is not a new concept at all. It has been used by some companies for years to reduce costs by improving internal workflow processes. The current interests in this topic are because of its potential applications in e-commerce. An E-signature can be as simple as a typed name individuals attach to an e-mail or more sophisticated as a digitized image of a signature that linked to a mathematical algorithm that verifies the authenticity of an on-line document; the signature is broken and invalid if the signature is altered after signing. The author provides a good account of the potential of electronic signature in on-line transactions especially those combine with digital certificate and smart card technologies, however, we must bear in mind that heckers are attracted to new challenges. Technology alone will not solve the problems facing electronic signature, a strong internal control system is required since most the security frauds or failures are mainly due to human factor.

Uday O. Ali Pabrai (2004) presents the business applications of electronic signature. He argued that by eliminating the inefficiencies of paper and its routing to customers, an organization can immediately capture a customer’s commitment to contracts and agreements instead of waiting days or weeks for the business opportunity to be realized. Electronic signatures may be used for electronic approval if:

- it combines cryptographic functions of a digital signature with the image of the person’s handwritten signature

- it authenticate data i.e. each time the document is opened an electronic signature automatically verifies and detects if data has been changed
- it provides secure authentication by referencing to digital certificate

A digital signature is commonly used as a part of an electronic signature solution. A digital signature is a cryptographic algorithm using private and public keys issued by the same certificate authority (CA). The author provided several questions that need to consider in choosing a vendor solution. He also argued that security professionals and architects must better understand, in particular, the associated standards and legislations, the applications and related technologies of electronic signatures.

Marcel Halpern (2001) predicts that legitimizing electronic and digital signatures by the US government has moved e-commerce one step forward and the Chief Information Officer (CIO) of an organization has to decide whether to use simple electronic signature or the more secure costly digital signatures. An electronic signature broadly defines under the e-Sign Act as “an electronic sound, symbol or process” executed or adopted with the intent to sing a contract or record. The author argues that major differences between different types of electronic signatures are security and authentication. At the low-end of security spectrum are click-through agreements, plain-text blocks at the end of an e-mail message, and user name and password combination. Clearly the author attempts to promote digital signature technology and considered some of its drawbacks. However, the article does not discuss the various types of internal controls to complement the digital signatures technology. Ren, Y.et al.(2015) propose a critical segment based verification system that aims to secure mobile transactions using user's behavioral traits. This is done using a combination of geometrical layout of signature and physiological characteristics demonstrated by user.

InterForum White Paper (1999) argues that the main challenge of electronic commerce is to understand the technology which underpin it and make it all possible. Cryptography is one of the key technologies, which allows users to have confidence and trust in the origin, the integrity, privacy and the confidentiality of messages they receive. To succeed, E-commerce must replace paper-based signature with a trusted digital alternative. Electronic signatures use a technology called public key cryptography. A user has a public key that is made available either through directories or via the web, and a private key. Public Key Infrastructure (PKI) provides the necessary trusted environment for efficient electronic working within and between businesses using digital signature. The paper does not differentiate between electronic signature and digital signature. At the same time PKI is more than just software, hardware, tokens, and networks; a PKI must conform to international standards that require regular and on-going audit. An audit framework for PKI is required to ensure the selected PKI solution meets conform to benchmarks of system security. PKI is still very costly and complex to implement, businesses interested in this technology must weigh the costs and benefits of its implementation.

2.3 Internal Control

COSO (1992)**,** Committee of Sponsoring Organizations of the Treadway Commission lists five interrelated components of internal controls:

a. *Control environment* - the foundation of for all other components of internal control, providing discipline and structure for integrity, ethical values and competence of the organization's people.
b. *Risk assessment* - the identification and analysis of relevant risks to achievement of the organization's objectives by forming a basis in managing risks.
c. *Control Activities* **-** policies and procedures to ensure management directives are carried out at all levels and in all functions of organization to address the risks.
d. *Information and Communication* - internal and external information must be identified, captured and communicated timely to run and control the business.
e. *Monitoring* - the process of assessing the quality of system's performance over time by reporting deficiencies to the relevant level of management.

Although COSO stated clearly the ways and roles and responsibilities of all the stakeholders in internal control, it is really a framework and its effectiveness will depend heavily on the organization's ability to execute the recommendations.

Task Force on Internal Control of The Institute of Internal Auditors Malaysia (2000**)** provides a guideline for all directors in public listed companies the key areas that directors must pay attention to before they make a statement about the state of their company's internal control. The Guideline pointed out the need for proper risk assessment which is a critical component of a sound internal control system.

Appropriate risk assessment, evaluation framework and activities are required for internal control to manage and control. Chou, E. Y. (2015) observes that they lack in the symbolic value of unique handwritten signature cherished by people and are unable to invoke person's presence and weight in subsequent decision making. These result in ineffective curbing of individual dishonesty and cheating.

COBIT Steering Committee (2002) issues the Control Objectives for Information and Related Technology (COBIT) framework to help management to bridge the gaps between business risks, control needs and technical issues. It provides best practices across a domain and process framework and presents activities in a manageable and logical manner. Management needs to put in place an internal control system or framework to support business processes, clearly defines how each control activity satisfies the information requirements and impacts the IT resourcesAn IT control objective is defined as "a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity." (Institute of Internal Auditors Research Foundation, 1994) Management has to decide the reasonable investment for security and control in IT and how to balance between risk and investment in control in an often unpredictable IT environment. Peter Plant (1998) discusses the importance of internal control and internal audit. Sound internal controls are essential in any organization to ensure the orderly and efficient running of a business. Corporate governance requires directors to ensure that an effective internal control system is in place. Internal control comprises the control environment and control procedures. An internal control system attempt to ensure: 1) complete and accurate accounting records are kept; 2) company assets are safeguard; 3) errors and/or fraud are prevented and detected if occur; 4) information is prepared and disclosed in timely and informative manner; 5) staff adhere to the policies and procedures; and 6) adherence to statutory and other relevant regulatory requirements.

William Hillison, Carl Pacini, and David Sinason (2001) discuss that control systems must be implemented in view of the explosive growth of electronic transactions to ensure security of assets, and integrity of information and transaction process. However, no single control procedure is appropriate for all types of transactions, events, or contracts. Absolute control is very expensive, if not impossible, to implement. The purposes of internal control are to: a) provide cost-effective measures against unauthorized access to or use of data; b) ensure reliability of financial records and accounts; and c) ensure compliance with applicable laws and regulations. Advances in digital signature technology require a continual evaluation of related control methods.

Noncryptographic controls are used mainly to mitigate identification and authentication risks. Examples of noncryptographic controls are password, personal ID number (PIN), and smart card, digitized handwritten signature. Biometrics technology which utilize unique physical characteristics of a person ─ voice patterns, fingerprints, and retinal patterns ─ provides very high levels of authentication but require privacy assurance. Cryptographic controls which use key(s) for encryption and decryption can control authentication, non-repudiation and security risks. Every digital signature is unique to the document for which it was created, preventing a forger from digitally signing a document or substituting one document for another.

2.4 Electronic Signature Technology

Julian Ashbourn (1999**)** provides a broad overview on biometrics technology, their usage, and performance measurement, how the systems are constructed and practical implementation issues. Personal identification number or PIN was one of the earliest techniques used to offer automated recognition. However, it is not able to recognize the person who presented it. The same is true for cards and other tokens. A biometric cannot be easily transferred between individuals and represent a unique identifier. It is considered more accurate and secure because biometric devices are not easily fooled. The technology is expected to be in widespread usage in commercial areas such as ATM machine use, workstation and network access, travel and tourism, Internet on-line transactions, telephone transactions, and public identity cards.The author gives an insight to the development of biometrics technology. Biometric authentication technology provides a substantially greater security than traditional passwords, PINs, and PKI security mechanisms. It also moves the security focus on preventing intrusion from within the organization which is the main source of unauthorized access to information. Its broad consumer acceptance and usage also depend greatly on price of implementing and maintaining this type of system, extensiveness of implementation, social acceptance, liability issues if lost or stolen, and establishment of administration and/or issuing authority.

IDynta White Paper (2002) focuses on the various applications of fingerprint biometric technology to provide a higher level of security for information access via Intranets, Extranets, the Internet, physical access and for more secure financial and e-commerce transactions. Authentication method is based on approaches or combination of: a) proof by knowledge ─ password, PIN number, or personal information such as a person mother’s maiden name; b) proof by possession ─ a card key, smart card, passport, optical card and token; and c) proof of property─ a biometric ─ the most secure and convenient authentication tool. A biometric cannot be forged, stolen, forgotten or borrowed. Biometrics technology uses the individual’s unique physical or behavioral characteristics to recognize or authenticate his/her identity. The most common physical biometrics includes fingerprints, hand or palm geometry, retina, iris or facial. Behavioral biometric characteristics include signature, voice, keystroke pattern, and gait. The paper discusses the benefits of fingerprint authentication in a wide range of industry sectors. Although biometric authentication provides a greater level of security environment, but incompatibility among these methods is limiting their usage. Interoperability among different vendor's solutions is an essential to enable broad consumer acceptance. Bartley et al(2016) observed that the web based transaction management environment enabled execution of multi-party electronic transactions by obtaining multiple handwritten signatures in real-time basis using simultaneous execution environment.

Tao Zhou (1999) discusses the use of digital signature technology in an electronic commerce environment where exchanging of documents over the Internet is very common. A digital signature on an E-commerce document helps to guarantee data origin, integrity, and non-repudiation. Digital signature technology grew out of public key cryptography. Basically, public key encryption or asymmetric encryption uses two different keys ─ a public key and a private key ─ to encrypt and decrypt a message e.g. e-mail. Fritz Grupe, Stephen G. Kerr, William Kuechler, and Nilesh Patel (2003) discuss the technology and impact of digital signature technology to businesses. They establish that digital signature technology not only help to improve workflow efficiency between transacting parties but also provide specific opportunities to improve internal control and the authenticity of data. It is essential that electronic, legally binding documents and transaction records are subject to a trustworthy process. Digital signature fits in the roles by providing authentication of identity, authorization, data integrity, non-repudiation, auditing, confidentiality or privacy, and availability. Digital signature is viewed to be more secured then traditional handwritten signature because document need to be digitally signed using a private key and verify using the sender's public key. Although the authors provide some guidelines to improve the internal control systems by recommending some changes to the existing practices, however, the guidelines are general and brief. The accountants or auditor must be aware of the organization's business objectives and must weigh the costs of implementing a control against the potential benefits of that control. A clearly written risk management framework would definitely helps the auditors in reviewing the implementation of digital signature.

Robert L Scheier (2002) predicts that widespread adoption of digital signature will be slow for the future because of the cost and complexity of the public key infrastructure (PKI) and the legal muddle over what constitutes a binding digital signature. According to Gartner Inc, "e-signature" is a generic term covering any electronic signing of a document including the digital capture of an actual signature, clicking on "yes" or "I agree" buttons to "sign" a document or agreement, or checking biometric characteristics such as fingerprint. In contrast, the digital signature uses a pair of mathematically related signing keys to verify the sender or to verify the content of the signed document has not changed during transmission. Digital signature provides non-repudiation i.e. neither sender nor receiver can later claim the transaction did not take place which is an important requirement when dealing with contract or sales of goods over the Internet.

American Bar Association (1996) provides a legal overview of the use of cryptography, digital signatures, and entity authentication over the Internet. Although a signature is not part of the substance of a transaction but it serves as evidence, ceremony, approval, and efficiency and logistics The costs of implementing digital signatures are: 1) institutional overhead i.e. the cost of establishing and utilizing services such as certificate authorities, and ensuring quality in performance, and 2) product costs i.e. costs related to hardware, software, licensing, and service. The benefits of digital signatures are: 1) minimize the risk of impostors; 2) minimize the risks of message corruption by tempering or altering; 3) strengthen the formal legal requirement for signature, writing, and original document since digital signatures are functionally on par or more superior then paper form; and 4) can send through any communication channels and still maintain high degree of information security.The author concludes that by analyzing its cost and benefits, digital signature is more superior than other forms of signatures e.g. paper signatures, digitized images of signatures, etc. However, the author did not discuss the degree of acceptance of digital signature in the commercial world. Watanabe (2015) identified that a new technology is proposed that enables confirmation of contractor consent in the block chain records of contracts.

2.5 Risk Management

Stephen A. Moscove (2001) discusses 4 types of risk associated with e-business: 1) information technology infrastructure, 2) user identification and authentication, 3) privacy, and 4) destructive computer programs. Glover, Liddle, and Prawitt defined e-business as the use of information technology and electronic communication networks to exchange business information and conduct transactions in electronic form. E-business operations represent a unique set of risks, including an increased reliance on technology and increased vulnerability to the rapid changes in technology. A cost-effective e-business internal control system should be developed and implemented toward the goal of reduced operating expenses and therefore increased profits.

One of the risks for e-business organizations is the theft of electronic data by internal employee and hackers and poor password administration poses the greatest risk. The author advocates that physical access control procedures, password control procedures, data encryption using public key infrastructure (PKI), and software-based security control procedures like firewall and intrusion detection system should be incorporated to control IT infrastructure risk. The risks of email spoofing, IP spoofing, fake websites can be controlled by adopting digital signatures and certificates which establish identity of a party to an e-business transaction. Biometric identifications which use distinctive physical characteristics (such as voice patterns, fingerprints, facial structure, or signature dynamics) can also be used to reduce the risk of falsified identity within e-business. Because every organization is unique (whether doing e-business or not), there is no standardized package of control procedures that work best for all. An optimal control package must balance the costs and the benefits of its specific application. A cost-benefit analysis should be performed on every perspective control procedures.

IDG New Services (2001) reports that humans is the weakest link in securing information systems as discussed in a security conference organized by Computer Security Institute. Security professionals must go beyond technology and engineering to protect a company's digital information. Computers cannot protect, only people can protect. A company's chief financial officer builds layers of controls around handling money like making more than one person sign checks or hiring outside firms to perform audits on accounting books, the same attitude should be applied when protecting a company's data. Existing security policies that do not make sense must be challenged. Securing company information is not just the job of security manager, it is everyone job. The report also pointed out that understanding the human component, or identifying who is behind the keyboard is essential to solving information security breaches. The report touches on one important aspect of security management often neglected by many i.e. human aspects. A company may implement the best technology to secure the information but it can be compromised by human.

Carl Ellison and Bruce Schneier (2000) discuss 10 risks of PKI not told by the vendors. Security is a chain; it is only as strong as the weakest link. The security implementation by any certificate authority (CA) is based on many links but not all of them are cryptographic. Trust is the forerunner of any CA-based security system. CA is taught to be trusted but this may be a myth then real. One of the biggest risks in any CA-based system is the private key, which is stored on a conventional computer. However, the computer itself is subject to the risk of attack by viruses or malicious programs. The authors do not answer how these risks could be avoided and mitigated if the use of PKI is unavoidable. An PKI audit framework may be warranted.

Bennett Gold (2001) discusses the complexity of modern enterprises with heavy reliance on technology and the heightened interconnectivity among organizations engaging in electronic business can be exploited by internal and external perpetrators within seconds. According to KPMG's 2001 Global e.fr@ud.survey security in credit card numbers, system availability, confidentiality of customer and company information, and maintenance of the integrity of this information are the major concerns in e-business initiatives. Less than 35% of the respondents have security audits performed on their systems. Management can be misinformed about the vulnerabilities of their network systems by 1) poorly trained and/or poorly qualify system/network administrators; 2) weak internal/implementation controls; 3) poor reporting procedures for security breaches; and 4) dishonest employees. The survey pointed out the increased use of encryption technology in e-business.

The report is based on a survey on 1,253 companies all over the world. The report clearly stated the importance of IT governance to control and manage technological risks related to e-business. The report does not recommend any particular IT governance framework to follow e.g. COBIT and elaborate how IT governance can assist in managing risks associated with e-business.

2.6 Issues managing digital information and its security

Zahri Yunos and Ahmad Nasir Mohd Zain (2004) discuss issues in managing digital information as a result of rising security demands of documents transferred over the Internet. Among the issues are:

a. Integrity of documents - the safeguarding of the accuracy and completeness of a digital document and its processing methods;
b. Confidentiality of documents - ensuring that the digital document is accessible to authorized users.
c. Availability of documents - ensuring that the digital document is made available to authorized users when required

The possible solutions to the above issues are:

a. Digital signatures technology - the use of private and public key pairs to verify whether a message has been altered en route has gained widespread acceptance in electronic commerce. Uncertainty to the legal status of the digital signatures can be a hindrance to e-commerce, since it makes the legal consequences of commercial activities over connected networks unpredictable. Various countries and international organizations had formulated legislation, regulations, and guidelines on digital signatures. In Malaysia, the digital signature technology must comply with the Digital Signature Act of 1997.

b. Time-stamping server – a service that enables Internet transactions, electronic documents or signatures to be signed with trusted time. The recording time is provided by a centralized stamping server to provide undeniable proof that digital data was not modified or backdated i.e. non-repudiation of documents.

c. Hardened operating system – a three-factor authentication using smartcard activation password, a smartcard with a digital certificate and biometrics provide state-of-the-art authentication that is superior then conventional username-password logins to computer terminals.

d. Digital watermarking – this helps to control the distribution of documents by providing ownership rights protection, authentication (visible and non-visible), various information access controls and information tracking.

3.0 Research Methodology

The research design for this study is based on secondary sources based on information gathered from various business magazines, journals, white papers, text books and Internet. The research framework for discussion, analysis and finding is shown in the following diagram: –

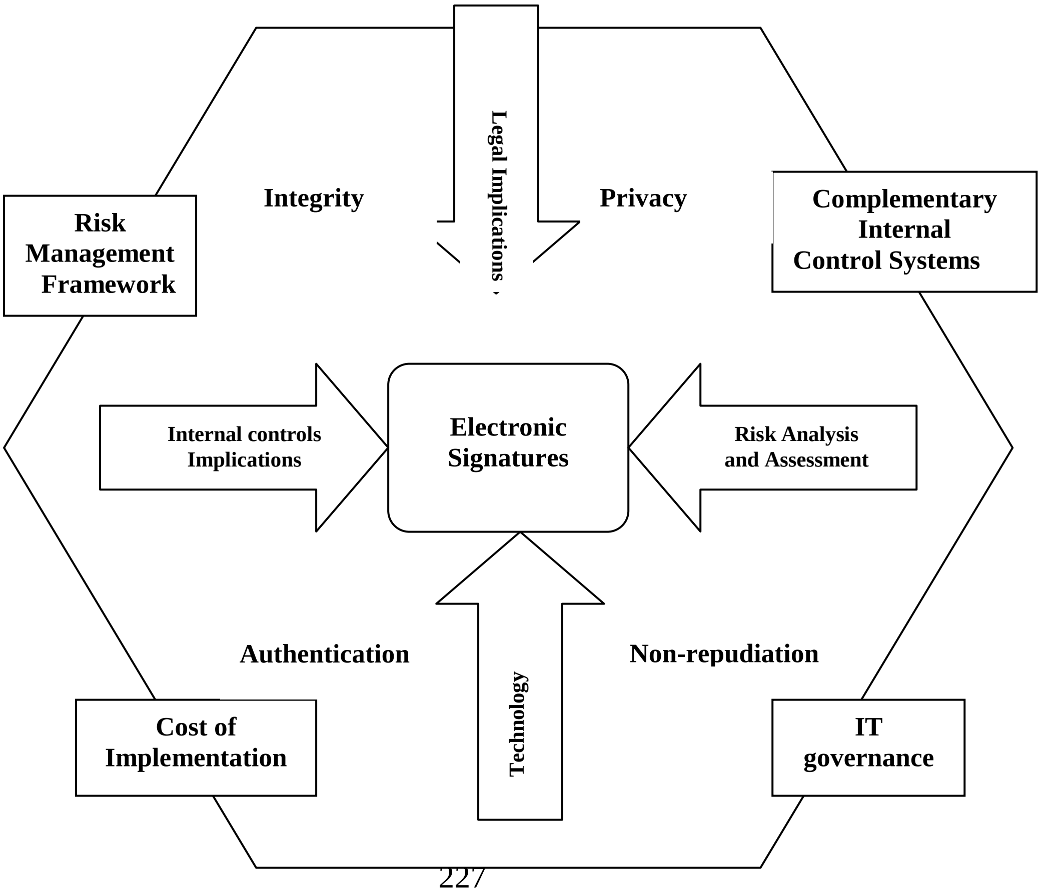

Figure 1: Research Framework

4.0 Discussion, Analysis and Finding

4.1 *The Need to Develop a Risk Management Framework for Electronic Signature*

The use of electronic signatures especially digital signatures helps to strengthen trust and confidence in paperless environment where information and documents, financial transactions or personal information are transmitted in a secure manner. However, it also entails potential risks, some of which are known and understood others are known but less understood, and still other are unknown. Zefferer, T., & Teufl, P. (2015) have stated that e-government services in Europe deploy eID and eSignature concepts for secure and usable transactions and there is large scale usage of mobile eID and eSignatures in several European countries in both public and private sectors. However, due to large variations in technology and organizational aspects, the hetergenous ecosystem results in insufficient insights. This study proposes a framework for effective and efficient adoption of mobile eID and e-signature solutions. It is thus important for businesses and management to identify, quantify, and manage the risks associated with electronic signatures. The risks in implementing electronic signatures include: ─

a. ***Strategic risk***
   This type of risk arises when overall implementation of electronic signatures or the chosen business model to support the electronic signatures is not in congruent with the vision and objectives of the business. This risk is usually the result of lack of senior management commitment to drive the electronic signatures implementation and left it to the technologist.

b. ***Operations risk***
   The reliance on electronic signatures to provide authentication, integrity, non-repudiation, and confidentiality makes security and internal control the main operations risk. Operations risks include inaccurate forecast of bandwidth requirement to support the electronic signatures, poor internal control system, and ineffective in managing intermediaries such as certificate authority. People is the weakest link in any security system, hence appropriate internal control procedures must be put in place to restrict the access to PC or token on which the electronic signature is stored.

c. ***Transaction risk***
   Very often an electronic commerce application or electronic payment system is linked to the back-end legacy system to allow for straight-through processing of electronic transactions. Such straight-through processing helps to reduce human errors, but it also increases dependence on sound system design and architecture. A poor system architecture, implementation or ineffective monitoring can result in fraud, errors in transaction and causing the transaction to be repudiated or dispute among the trading parties.

d. ***Security risk***
   This risk can be classified into: ─
   a. Privacy and confidential risk ─ the risk where electronic message may be read or visible to or accessed by unauthorized parties.
   b. Integrity risk ─ the risk where the data transmitted is altered or modified deliberately or inadvertently compromising the accuracy of data, integrity of transactions and confidence of the trading parties.
   c. Authentication risk ─ the risk in which the identity of a party to a transaction may not be what he claimed to be.

d. Repudiation risk ─ the risk where a trading party may dispute or deny the validity or refuse to acknowledge legitimate communications and transactions.
e. Access control risk ─ the risk where an unauthorized person can gain access to the system, network, operating system or application that could lead to fraud in transaction, alternation of data, data confidentiality, etc.

e. ***Legal risk***

Electronic signature carries heightened legal risks for companies who implement it. The borderless nature of the Internet allows a company to do business globally. However, laws are territorial in nature and in some cases companies might not be fully aware or understood the local jurisdiction of local laws and regulations before they offer the electronic signature services. As a consequence, a company could unknowingly violate customer protection laws including on data collection and privacy, and regulations on soliciting.

f. ***Reputation risk***

Reputation risk can be caused by failure or unreliable services provided by an electronic signature implementation resulting in widespread negative reaction on the company in the marketplace by its customers, business partners, or general public. The more a company relies on electronic signature for its electronic authentication, the greater is the potential risks. This risk potentially can result in financial losses to the company if customers question the validity or refuse to acknowledge legitimate communication or transaction.

g. ***Compliance risk***

These are risks associated with violation of laws, rules, regulations, prescribed practices or ethical standards which can result in loss of customer confidence in using the electronic signature, non-enforceable contract or loss of business.

h. ***Technology risk***

The main concern of electronic signature is over reliance on some security protection mechanisms like encryption. In PKI implementation, if the security key is compromised, a company stands the risks of unlimited liability. Similarly an electronic signature implementation that is on the low end of security spectrum can be compromised easily. Likewise software bugs are prevalent in browser, Java engine, operating system or application system.

In designing an effective Risk Management Framework for electronic signatures, it is important to first consider the types and values of business information need to be protected before embarking the project. The selected implementation of electronic signature must be best suited for a given situation to meet the control objectives required. The principles and control criteria established in *Internal Control – Integrated Framework* by COSO (1992) could be used as a guide in developing the Risk Management Framework for electronic signatures. The five inter-related components of effective internal control proposed are:

1. Control environment;
2. Risk assessment;
3. Control activities;
4. Information and communications; and
5. Monitoring

4.2 Risk Management Practices in the wake of e-signature

The company should also put in place effective risk management principles or practices to identify, monitor, control, and prevent or mitigate potential risks of electronic signatures. The risk management principles should cover at least the following areas: —

a. ***Strategic planning analysis*** **—** the implementation of electronic signatures must be in-line with overall business objectives and operating model.

b. ***Risk identification, assessment and monitoring*** **—** all risks related to electronic signatures must be properly identify, quantify, and measure. Assessment of the impact to the business and internal control systems must also be made. An integrated risk management approaches such as those proposed in COBIT (2000) may be adopted. A Risk Management Scorecard using Balanced Scorecard principles may be used for on-going reviews and monitoring.

c. ***Technology implementation*** **—** internal control policies and procedures, training, testing, contingency planning, and selection criteria for the right mix of technologies and usage of intermediaries must be established before implementing any electronic signature.

d. ***Authentication management*** **—** should have a formal written security policy, standards and procedures to ensure trust and confidence in using the electronic signatures. Management must put in place a combination of critical technologies and access control policy and procedures to secure access to the networks, IT systems and application systems. In addition, policy on the usage of cryptographic controls for the protection of critical/sensitive information when store or transmitted over communication networks must be established.

e. ***Audit and review*** **—** regular objective review must be conducted on the implementation of electronic signatures to identify and quantify risks, to review adequacy of internal controls procedures, policies and processes, and to detect possible weaknesses in the risk management program.

f. ***Staff and expertise requirements*** **—** management must identify the staffing level, the training needs, and skill sets to support the electronic signatures implementation.

In short, management is able to promote trust and confidence of people in using the electronic signature to do business with the company. In addition, company should educate its customers on their rights and responsibilities in protecting their privacy and integrity of information. The customers may be required to have agreement on the terms and conditions before using the system. At the same time, management should develop necessary internal control procedures to safeguard customer information including creating privacy policies and procedures and ensure the staff abides with the privacy policies as part of the company's corporate culture. Bartley Joshua et el.(2016) have observed that the web based transaction management environment enables execution of multi-party electronic transactions by obtaining multiple handwritten signatures in real-time basis using simultaneous execution environment.

4.3 *Cost Consideration in Implementing Electronic Signatures*

The main obstacle in electronic signature implementation beside security is cost. The implementation must meet the business mission and objectives. There must also have ROI for such technology implementation. In many cases, the implementation of electronic signature especially with digital signature using PKI would require business process re-engineering. Rarely can digital signatures simply be "plugged in" or "switched on" without any adjustment. Businesses have to decide how to secure electronic transactions and customize existing legacy or on-line applications to accept and store them. This may require substantial investment. Similarly it may require client or business partner to invest in physical devices such as smartcard reader or USB-based token. Rath et el.(2015) found that the use the obligatory two factor user-authentication - of eID and eSignatures, have gained popularity for e-Government solution transactions, especially in Europe. While cost effective, the typical one-time SMS technology used for this purpose is considered insecure. The proposed alternative user-authentication system, based on challenge-response approach is shown to address both cost and security requirements, as validated by the results of two implementations of the proposed system.

The cost of implementing electronic signatures will depend on the levels of trust an application is required to provide. The security services in a trust model include data integrity, privacy, authentication, non-repudiation, and access control. The higher the level of trust is required, the more complex form of electronic signature such as digital signature with Public Key Infrastructure (PKI) or biometric technology will be employed, and the greater is the cost of implementation. In determining the implementation costs for any electronic signature, the management should consider the following factors: ─

- the nature of the transactions (e.g. number or frequency, amount of information transferred, value of the information etc) especially those containing financial information, customer information that requires privacy, proprietary business confidential information, contracts, etc.;
- regulatory and statutory requirements such as those required by Bank Negara Malaysia;
- the level of assurance given by the current application without any electronic signature that warrant changes;
- the network infrastructure especially bandwidth requires to support the electronic signature;
- the scope of application, especially when growth that creates financial impacts or other pressures that more secure electronic signature like digital signature can better address;
- the maturity of a particular type of electronic signature;
- process reengineering;
- business continuity plan;
- interfaces to other legacy applications – internal and external;
- the user expectations and user profile including amount of user education needed; and
- market acceptance for the technology.

Depending upon a particular situation and the way organization implements its risk mitigation program, an organization may be able to define possible financial impacts by extrapolating losses due to fraud or computer crime without electronic signatures. It is important to identify and quantify all the potential benefits of electronic signatures so that a fair comparison of costs and risks can be made. Some of the potential benefits of electronic signatures are: ─

- *Time savings* ─ electronic signature and electronic process can reduce the cycle time required to process information thus increase responsiveness of an organization;
- *Cost savings* ─ the cost of reduction is derived from decreased transaction time, improved operational efficiency, reduce cost for storage, printing and papers, increased accuracy and productivity, reduced maintenance costs associated with paper-based systems, and better and more efficient way for customers to pay for services rendered or products purchased.
- *Enhanced service* ─ the ability to provide availability and accessibility of business processes to internal users as well as external users is enhanced. The strong authentication, which digital signatures or biometric technologies provide, allows the organization to provide broader services and reach a greater number of audiences that traditionally may not be cost effectively to serve. With the growth of Internet and increase sophistication in the use of electronic processes and information and communication technology (ICT), electronic accessibility with electronic signature provides an opportunity to do business and communicate with each other in a more secure manner any time, any where, and using any device.

4.4 ***The Need to Develop an Internal Control System to Complement Electronic Signatures***

Every company needs some forms of controls to regulate their business activities. The professional accountancy and audit grew out of needs for owners or shareholders to regulate the behavior of those helping them to run the companies. In developing an effective internal control system to supplement the built-in controls by electronic signatures, the principles and control objectives established in *Internal Control ─ Integrated Framework* by COSO (1992) may be adopted. COSO defines internal control as a process effected by a company's Board of Directors and senior management. The controls must also be cost effective, therefore a cost/benefit analysis must be done when designing and evaluating control process even though it is not always easy to quantify the benefits and matching the best control to the risk of loss (William Hillison, Carl Pacini, and David Sinason, 2001).

While some implementations of electronic signatures such as biometric and digital signature using PKI can create a trusted environment that promote the use and growth of electronic processes, an effective internal control system must be also developed to complement the electronic signature. This includes the creation of policies and procedures to protect the usage of and access to electronic signatures, segregation of duties between operations and application development staff, turning on audit logs on critical processing, regular audit on PKI service provider and certificate authority. A methodology must be developed to assist management to measure the effectiveness of the organization's internal control system for electronic signature. Some organizations used Risk Management Scorecard as a mean to review the effectiveness of an internal control system and risk mitigation program. It also allows the management to measure improvements in internal control system and to tune it for overall cost-effectiveness. Fabritz et al.,(2016) have analyzed that digital signatures are one of the most attractive solutions in the computerized message systems to address the issue of lack of trust between the sender and receiver. In addition, they eliminate mundane, manual labour required for physical verification and thus provide higher degree to assurance and authenticate online and mobile transactions.

To establish effective controls for electronic signatures, an organization must conduct risk assessment on the environment in which it operates. Specifically the results of the risk assessment can be classified into:

- Risks which must be guarded against;
- Risks which have either low impact or low probability of occurrence where no specific internal controls are needed; and
- Risks where the financial impacts can be transferred to another organization like insurance companies. For the risks to be transferred, an organization is required to implement controls that meet the requirement of insurance policy.

The classification clearly shows that not all types of risk in electronic signatures require an equivalent internal control system. Risk that does not have direct impact to financial transaction or privacy of customer information can be mitigated by implementing a simple internal control procedure. However, the question remains, "How does the company know when the loss is insignificant?" Surely, the company is at risk if it cannot answer this question satisfactorily. While eSignatures represent both convenience and efficiency, and perform similar objective functions, Chou, E. Y. (2015) pointed that they lack in the symbolic value of unique handwritten signature cherished by people and are unable to invoke person's presence and weight in subsequent decision making. These result in ineffective curbing of individual dishonesty and cheating.

To overcome this, there are three classes of internal controls which a company can implement:-

- Preventive ─ which seek to ensure the impact is never materialized. This type of control seek to prevent an event from happening or affecting the organization in terms of financial, legal or reputation, or detects the event as it happens and prevents from further impact;
- Detective ─ which identify the occurrence of an event that leads to realization of impact and apply appropriate action to arrest it; and
- Reactive ─ recovery action after the occurrence of an event resulted in an impact.

However, not all events can be detected internally by the organization. Some events may be detected by other stakeholders such as customers, suppliers, business partners, employees, etc when they lodge a complaint to the organization or repudiate an electronic transaction or refuse to honor a contractual agreement. An effective internal control system should incorporate an incidence response system to identify the cause of complains and makes necessary corrective action. Controls do not always work as intended and do fail from time to time. Over dependence on technology such as PKI or certificate authority to provide authentication in digital signature implementation is a risk by itself. Management should have an audit framework to conduct regular review on the management of the selected PKI services.

Quality control is a critical component of any internal control system. The thrust of good software engineering techniques that involve electronic signature technology is generally towards detecting errors as early as possible during the development life cycle. However, a good quality system involves cost and the cost must be balanced against the cost of failure. There is a trade-off between cost and quality and a similar trade-off between cost and internal control system. What is important to the management is that the internal control system must complement the controls created through electronic signature to meet the business objective of build a trusted and secured environment for electronic processing. Clearly written polices on the usage of electronic signatures must be communicated and enforced. Lastly designing the most effective internal control system for electronic signature implementation would require a balancing act between the cost and benefits derived.

4.5 Future scenario of Digital Signatures

The future of e-signature or digital signatures is briefly presented below.

a. Confidentiality of group digital signatures is ensured by using proposed public keys encryption algorithm (Ambedkar, B. R.et al.2016)
b. During electronic transactions between consenter and consentee, the pool proof method and system will exist by display of a unique code in the screen of a digital video to verify that the consenter is alive.(Williams, S. E., & Williams, J. F.2016)
c. A novel digital signature schemes will be introduced based on factoring and discrete logarithms to prove the security of digital signatures.(Chiou, S. Y. 2016)
d. To speed up the operations involving digital signatures, enhanced digital signature using RNS digit exponent representation will be installed in line with modern processors. (Plantard, T., & Robert, J. M. 2016)
e. The hybrid cryptography is adopted to reduce the network created overhead caused by digital signature.(Salvi, D.et al. 2016)
f. Significant ongoing research is done in areas of quantum digital signature (QDS) that borrows its establishment from essential laws of quantum physics. Advancement in areas of QDS promises to remove the supposition of authenticated quantum channels though remaining secure against collective attacks (Yin & Chen, 2016).

5.0 Limitations

Given the limited time for this research on the impacts of electronic signatures on internal control systems, the study is limited by lack of literature related to the subject matter, and lack of local scenario and case study. A detail study is required to examine various variables that may affect the relationship between electronic signatures and internal control systems. Because of the time limitation of this research, this paper did not discuss the methodology that can be used to measure the effectiveness of an internal control system, but focus on the need to develop a cost-effective internal control system to complement the electronic signature implementation. This paper also did not discuss in details the formulation of a Risk Management Framework to mitigate the risks of electronic signature. Furthermore, the research does not study the market acceptance of electronic signature in Malaysia. It is suggested that further research to be done to collect and analyze the data on the implementation of electronic signatures in Malaysia and their impacts to the internal control systems in various industries.

6.0 Conclusion

There are many risks associated with electronic signatures and not all of them created equal. The business objectives of a signature are to provide attribution, affirmation, authentication, and non-repudiation. Digital signature is one form of electronic signatures that uses PKI technology and appeared to be the most logical choice for E-commerce scenario. From the discussion and analysis, a formal clearly written Risk Management Framework should assist management to systematically identify, evaluate, quantify, assess, monitor and control the risks in implementing applications that make use of electronic signature technology. To manage, track and mitigate these risks, a Risk Management Scorecard using Balanced Scorecard format will help. Electronic signatures are normally part of the "e" initiatives in a company. It can also be employed in other forms of security implementation that do not go through Internet such as ATM, immigration checking, etc, The Risk Management Framework is applicable to any type of application that requires electronic signatures for security.

Despite legislations that recognize electronic signature to be on par with handwritten signature, heavy investment associated with advanced authentication infrastructures is one of the main obstacles for business world to adopt electronic signatures. The more secure a system, the more costly is the implementation of controls. As such, any decision to implement electronic signatures should be based on a thorough cost-benefit analysis. Management evaluating the cost-benefit analysis on electronic signatures should understand fully all the risks associated with a selected electronic signature so that cost considerations fully incorporate appropriate controls to mitigate the risks. Similarly, management should unearth all benefits that can be derived from a particular electronic signature technology.

The implementation of electronic signature should be complemented by an effective internal control system. A company must bear in that electronic signatures only help to answer part of the internal controls required in a paperless environment. Moreover, electronic signatures do not always work as intended. If this is not mitigated with an effective internal control system, it may potentially result in great financial losses to or legal actions against the organization or company.

In selecting an electronic signature technology to implement, companies need to evaluate whether the technology achieve what they wanted, cost and complexity of the technology, whether there is a need to push tools or techniques to the customers, who to place the trust on, and compatibility and interoperability of electronic signatures. Standards are required to ensure compatibility and interoperability of digital signatures. There are still bumpy roads ahead before we could see a wide acceptance and usage of electronic signatures in the electronic transaction environment.

References

Abbdal, S. H., Kadhim, T. A., Abduljabbar, Z. A., Hussien, Z. A., Yassin, A. A., Hussain, M. A., & Waley, S. (2016). Ensuring Data Integrity Scheme Based on Digital Signature and Iris Features in Cloud. Indonesian *Journal of Electrical Engineering and Computer Science*, 2(2), 452-460.

Ali Farhoomand with Peter Lovelock (2001), "*Global e-Commerce – Text and Cases*", *Prentice Hall*.

Ambedkar, B. R., Gupta, A., & Bedi, S. S. (2016). Confidentiality of Group Digital Signature Using Proposed Public Keys Encryption Algorithm. *International Journal of Engineering Science*, 2303.

American Bar Association (1996), "Digital Signature Guidelines Tutorial". *The American Bar Association*, December. URL: http://www.abanet.org/scitech/ec/sc/isc/dsg-tutorial.html .

Bank Negara Malaysia (2000), "Guidelines on Provision of Internet Insurance/Takaful by Insurers and Takaful Operators", *Bank Negara Malaysia*.

Bartley, Joshua A., and Maxwell J. Battcher. (2016) "E-SIGNATURE." *U.S. Patent 20,160,179,776*, .

E-SIGNATURE United States Patent Application 20160179776

Bennett Gold (2001), "Considering Security and Control", *The New Straits Times*, July. URL: http://www.e-commercellert.com/article311.html

Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014). Chip and Skim: cloning EMV cards with the pre-play attack. In 2014 *IEEE Symposium on Security and Privacy* (pp. 49-64). IEEE.

Carl Ellison and Bruce Schneier (2000), "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", *Computer Security Journal*, Volume XVI, Number 1.

Cem Kaner (1997), "The Insecurity of the Digital Signature", *Cem Kaner*, September. URL: http://www.badsoftware.com/digsig.htm

Chang, I. C., Hwang, H. G., Hung, M. C., Lin, M. H., & Yen, D. C. (2007). Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department. *Decision Support Systems*, 44(1), 350-359.

Chou, E. Y. (2015). Paperless and Soulless E-signatures Diminish the Signer's Presence and Decrease Acceptance. *Social Psychological and Personality Science*, 6(3), 343-351.

Chou, E. Y. (2015). What's in a name? The toll e-signatures take on individual honesty. *Journal of Experimental Social Psychology*, *61*, *84-95*.

Chiou, S. Y. (2016). Novel Digital Signature Schemes based on Factoring and Discrete Logarithms. *International Journal of Security and Its Applications*, 10(3), 295-310.

Grigg, D. M., Starbuck, R. A., Hanson, C. A., Jones-mcfadden, A. C., Dent, N., Munson, N., & Bryant, M. K. (2016). U.S. Patent No. 20,160,005,048. Washington, DC: *U.S. Patent and Trademark Office*.

Christopher Kuner, Anja Miedbrodt (1999), "Written Signature Requirements and Electronic Authentication: A Comparative Perspective".
URL: http://www.kuner.com/data/articles/signature_perspective.html

COBIT Steering Committee (2002), "COBIT 3rd Edition – Management Guidelines", *IT Governance Institute*, July.

COSO (1992), "The Internal Control – Integrated Framework: Executive Summary", *Committee of Sponsoring Organization of the Treadway Commission*.
URL: http://www.coso.org/Publications/executive_summary_integrated_framework.htm

Dagmar Bosáková (2003), "Development of Electronic Signatures", *EBSCO Publishing*

Daniel Uhlfelder (2000), "Electronic Signatures and the New Economy", *Higher Markets*

Dr. David Brewer and William List (2004), "Measuring the effectiveness of an internal control system", *Gamma Secure System Limited and W*^{in}*, List & Co.*
URL: http://www.gammassl.co.uk/topics/time/index.html

Efraim Turban, Jae Lee, David King, and H Michael Chung (2000), "Electronic Commerce – A Managerial Perspective." *Prentice Hall*

Fabritz, N., Falck, O., & Saavedra, J. C. (2016, April). Doing Business in Croatia. In CESifo Forum (Vol. 17, No. 1, p. 52). *Institut für Wirtschaftsforschung* (Ifo).

Fairchild, A. (2012). The Evolution of the e-ID card in Belgium: data privacy and multi-application usage. Proceedings of Sixth International Conference on Digital Society.

Fritz Grupe, Stephen G. Kerr, William Kuechler, and Nilesh Patel (2003), "Understanding Digital Signatures", *The CPA Journal*, June

George V. Hulme (2000), "E-signatures: Ties That Bind", *InformationWeek*, July

Gary P. Schneider and James T. Perry (2nd Edition) (2001), 'Electronic Commerce", *Course Technology*

IDG News Service (2001), "People 'Weakest Link' in the Security Efforts", *Bennett Gold*. Accessed on URL: http://www.securitymatters.com/newsheadlines-01.shtml

IDynta White Paper (2002), "Application of Biometric Technology Solutions to Enhance Security", *IDynta Systems Incorporated*. URL: http://www.idynta.com/whitepaper.htm .

InterForum White Paper (1999), "Electronic Signatures – Signing up to the Digital Economy", *InterForum*. URL: http://www.interforum.org

IT Governance Institute (2002), "COBIT 3rd Edition – Management Guidelines", *COBIT Steering Committee and the IT Governance Institute,* July

Julian Ashbourn (1999), "The Biometric White Paper", *Avanti – The Biometric Reference Site*. URL: http://www.avanti.1to1.org/whitepaper.html

Kathy Lyons-Burke (2000), "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication", *National Institute of Standards and Technology, Technology Administration, US Department of Commerce*. October

Marcel Halpern (2001), "Not All E-Signature Are Equal", *CIO,* January

Marilyn Greenstein (2000), "Electronic Commerce: Security Risk Management and Control", *McGraw Hill*

Rath, C., Roth, S., Bratko, H., & Zefferer, T. (2015, September). Encryption-Based Second Authentication Factor Solutions for Qualified Server-Side Signature Creation. *Proceedings of International Conference on Electronic Government and the Information Systems Perspective* (pp. 71-85). Springer International Publishing.

Peter Plant (1998), "Internal Audit and Control", *ACCA Student Accountant,* Nov.

Plantard, T., & Robert, J. M. (2016). Enhanced Digital Signature using RNS Digit Exponent Representation. *International Workshop on the Arithmetic of Finite Fields,* WAIFI 2016. Springer.

Rebecca A. Askew, (2004), "Understanding Electronic Signatures", *RealLegal,* May

Rao, K. K., & Yadav, S. K. (2016). Implementation of Cloud storage Security Mechanism using Digital Signature. *inpressco.com*

Rath, C., Roth, S., Bratko, H., & Zefferer, T. (2015). Encryption-Based Second Authentication Factor Solutions for Qualified Server-Side Signature Creation. *Proceedings of International Conference on Electronic Government and the Information Systems Perspective* (pp. 71-85). Springer International Publishing.

Ren, Y., Wang, C., Chen, Y., Chuah, M. C., & Yang, J. (2015, September). Critical segment based real-time E-signature for securing mobile transactions. *Proceedings of Communications and Network Security (CNS), 2015 IEEE Conference* (pp. 7-15).

Robert L Scheier (2002), "Digital Signature: Use with care, if at all", *Boylston*. February.

Robins, Kaplan, Miller & Ciresi (2000), "Electronic Signatures in Global and National Commerce Act (ESIGN) – *FAQs and Resource Links*". URL: http://www.rkmc.com

Salvi, D., Samant, R., Patil, A., Repale, M., & Sonawane, M. (2016). Prevention against Attacks in MANET Using Secure IDS. *Prevention,* 5(2).

Schroers, J., Van Alsenoy, B., & Cuijpers, C. (2015). Legal analysis of eSignature services.

Secretariat (2000), "Statement of Internal Control - Guidelines for Directors of Public Listed Companies", *The Institute of Internal Auditors Malaysia.*

Stephen A. Moscove (2001), "E-Business Security and Controls", *The CPA Journal*. URL: http://www.luca.com/cpajournal/2001/1100/features/f114001.htm

Suruhanjaya Komunikasi dan Multimedia Malaysia, "Digital Signature Act 1997", *Malaysia Ministry of Energy, Water and Communication*. URL: http://www.mycert.org.my/bill [accessed May 13, 2004].

Tao Zhou (1999), "Digital Signature Technology", *Penton Media,* http://www.winnetmag.com/Articles/Print.cfm?ArticleID=4772

Task Force on Internal Control (2000), "Statement on Internal Control – Guidelines for Directors of Public Listed Companies", *The Institute of Internal Auditors Malaysia*.

Todd Hartman (2001), “Making Sense of E-Signatures”, *Robins, Kaplan, Millier & Ciresi L.L.P.*, October. URL: http://www.rkmc.com

Uday O. Ali Pabrai (2004), “The Business of Electronic Signatures”, *Certification Magazine*, February

US State Department, “Section 4 – Glossary of Electronic Signature Terms”. URL: http://www.state.sd.us/standards/Section%2014-4.htm [

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. J. (2015). Blockchain contract: A complete consensus using block chain. *Proceedings of IEEE 4th Global Conference on Consumer Electronics (GCCE)* (pp. 577-578).

White Paper (2003), “Effective Internal Control of Sensitive Information”, *Sealed Media*. URL: http://www.sealedmedia.com

William Hillison, Carl Pacini, and David Sinason (2001), “Electronic Signatures and Encryption”, *The CPA Journal*. URL: http://www.luca.com/cpajournal/2001/0800/features/f082001.htm .

Williams, S. E., & Williams, J. F. (2016). U.S. Patent No. 20,160,042,481. Washington, DC: *U.S. Patent and Trademark Office*.

Yin, H. L., Fu, Y., & Chen, Z. B. (2016). Practical quantum digital signature. *Physical Review A*, 93(3), 032316

Zahri Yunos and Ahmad Nasir Mohd Zain (2004), “Securing Digital Documents”, *thestar online*, April.

Zefferer, T., & Teufl, P. (2015). Leveraging the Adoption of Mobile eID and e-Signature Solutions in Europe. *Proceedings of International Conference on Electronic Government and the Information Systems Perspective* (pp. 86-100). Springer International Publishing.