IIUC STUDIES
ISSN 1813-7733
Vol. - 6, June 2010 (p 111-122)

A Study of Digital Signature and Its Legal Implications in Context of Bangladesh

Mohammad Hasan Murad*

Abstract: *The exponential growth of Information and Communication Technology particularly internet has brought about a revolution in the way we do financial and commercial transaction. Electronic commerce opened the door to reach out to global markets. Business has transcended geographical or time limit. More and more, Governments, businesses and consumers are taking advantage of the fast and efficient ways of information technology to conduct commerce. The internet is being used to exchange information; products and services are being designed and marketed ,bought ,sold and even delivered to places which was unimaginable even two decades ago. The internet has helped to achieve true globalization. E-commerce enhances convenience and choice, promote competition, and above all, generate new business opportunities and market efficiencies. However , the growth of e –commerce posed a profound concern of security and authenticity of the transactions as internet is open to all and perpetrators are always out there. This concern called for security, authentication and identification measures on internet to prevent fraud and malicious transaction. The technology has responded to this concern by developing online authentication and identification technology namely electronic signature, principally, digital signature. In this paper I have explored the meaning, technology of digital signature and discussed legal issues of digital signature particularly in context of Bangladesh.*

Key words: *Digital signature, electronic signature, online authentication, certifying authority*

1. Introduction

Internet is a open platform of communication which makes it vulnerable for all kinds security threats for instance, hacking, data intervention, fraud and fishing etc. For e-ecommerce to accomplish its full potential, a new mechanism of identification and authentication

* Lecturer, Dept. of Law, IIUC

was required. Electronic signatures, in particular, digital signatures were established with the aim of identifying the parties and authenticating and facilitating commercial transaction in the electronic environment. An important issue relating to digital signature is the legal recognition of it so that it provides with the same assurance and trust that the traditional paper signatures usually offer. In order to achieve this standard a whole new legal framework was needed.[1] In many developed countries Electronic and Digital signature laws immerged in recent decades. A few developing countries also have attempted to give digital signature a legal form by enacting separate new legislation or by incorporating provisions relating to digital signatures in their Information Technology laws. However, in practice digital signatures opened a new area of debates as far as evidential issues and standards are concerned.

2. Digital signature and Electronic signature

Although terms, electronic signature and digital signature are sometimes used interchangeably there are differences between them. United Nations Commission on Trade Law (UNICTRAL) has formulated a Model Law on Electronic Signatures with Guide to Enactment[2] where section 2(a) defines electronic signature as "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." A digital signature is a type of electronic signature which is created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form.[3] As we can see from the both definition electronic signature is a wide concept and is technology neutral while digital signature is based solely on cryptographic technology. Electronic signatures can take the form of a digital signature, a scanned image of handwritten signature, a digitized fingerprint , retinal scan, a personal identification number(PIN) or merely a name typed at the end of an email. A digital signature is the most secure form of electronic signature which provides greater authenticity and reliability to the communication it is attached with.[4]

2.1The Concept of Digital signature

A digital signature is an electronic signature created and verified by using cryptography that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to

ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.[5]

From the above definition we can deduce three fundamental principles behind digital signatures just as with any kind of signatures. They are as follows:

a. *Authentication*-which is concerned with assurance of identity.[6] A digital signature ensures that the message attached to it is sent by the person intended to send.

b. *Data integrity* - assurance that data has not been altered since the signature was applied. A digital signature offers excellent service of data integrity as any attempt to alter the data message will result in altering the hash value and the document could not be opened by original public key[7].

c. *Non-repudiation*- which is concerned with offering evidence to a third-party , for instance a judge, that a party participated in a transaction, and thereby protect other parties in the transaction against false denials of participation[8]. Since a digital signature is highly secured and a message can only be read by using key pain the signatory cannot, at least in theory, deny that he has not signed the document.

2.2 Difference between a Digital Signature and Manuscript signature

The United Nations Commission on International Trade Law (UNCITRAL) describes the functions of the traditionally handwritten signature as follows: a signature is to identify a person, to provide certainty as to the personal involvement of that person in the act of signing, and to associate that person with the content of a document.[9] Digital signature and hand written signature share the same objectives but differ in many ways.

It is very difficult to measure the level of assurance the hand written signatures provide. Usually during the dispute of authenticity hand writing and signature experts are used to identify whether the signature is genuine. Professional forgers have been able to fool those experts. However, hand written signatures are continued to be used as they generally provide adequate security for the document they relate. There are also practice of notarizing and signing before witnesses for

increased security. It is far more complex process to judge whether a digital signature is valid.

A pen cannot be hacked to sign itself but a computer can be hacked or taken over by a malicious programmer and it is quite possible to get a document signed by the signature software in that computer without the knowledge of the owner. There are many documented instances of networked computers being manipulated by malicious "outsiders" to do things the legitimate user would never have approved.[10]

Another difference between handwritten and digital signatures concerns the mechanism of association between the signer and her signature. A handwritten signature is biologically linked to a specific individual, but cryptographic authentication systems bind signatures to individuals through technical and procedural mechanisms.[11]

2.3 Technology of digital signature

The technology on which digital signatures rely is called 'Public Key Cryptography'. The essence of public key cryptography is the public/private key pair often simply known as **the key pair**. This is a pair of cryptographic keys that have the interesting property that anything encrypted with the public key can only be decrypted with the private key[12] and anything encrypted with the private key can only be decrypted with the public key.

The usual practice is to keep your private key secret and known only to yourself and to allow the world at large to know your public key. It is vital to understand that it is unfeasible to figure out what the private key is, given the public key.[13] Public Key Infrastructure consists of four steps-

a. The first step is creating a private key which will be confidential and a public which is known to all who is interested.

b. The second step is for the sender to digitally sign the message by creating a unique digest of the message and encrypting it. A "hash value" is created by applying a "hash function" - a standard mathematical function - to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. The hash function is encrypted or scrambled by the signatory using the sender's private key. Asymmetric encryption provides one of the highest - if not the highest - degrees of security in electronic transactions. The encrypted hash function is the "digital signature" for the document.[14]

c. The third step is to attach the digital signature to the message and to send both to the recipient.

d. The fourth step is to decrypt the digital signature using the sender's public key. If decryption is possible then the signature is authentic.
In order to realize the full potentials of PKI the receiver of digital signature known as the relying party must be assured of authenticity of the public key. This is where Certification Authorities come in to play. They ensure that a particular public key belongs to the actual sender and issue a certificate in this regard and relying party of digital signature depends on such certificate. A certificate is a digitized record that contains, among other things, the address of certificate issuing authority, the user's public key and the digital signature. The whole process is clarified in the following illustration-

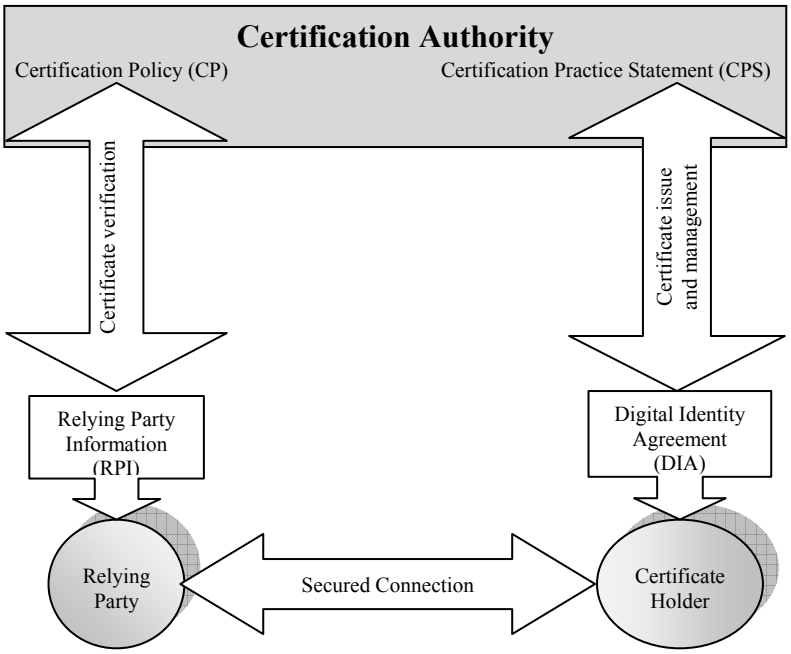

Figure 1[15] : Certification Procedure of Public Key Infrastructure

3. Recognition of Digital Signature in Bangladesh

As a signatory of World Trade Organization, Bangladesh has accepted the Code of Good Practice of the WTO Agreement on Removing

Technical Barriers to Trade.[16] As part of ongoing legal framework development in an attempt to keep pace with globalization, Bangladesh has enacted Information Technology Act in 2006. The object of the legislation, *inter alia* , is to facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce and to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.[17] It is evident that Information Technology Act 2006, hereinafter as The Act, has given legal recognition to digital signatures in order to bring digital signature under complete legal and evidential scrutiny.

3.1 Signature under traditional law

Signature is required by different laws to prove identity and intention. The word 'signed' is often used to denote a signature is put in proper manner on a document which is purported to be authenticated by such signature. According to Section 3(52) of General Clauses Act 1897 "sign", with its grammatical variations and cognate expressions, shall, with reference to a person who is unable to write his name, include "mark", with its grammatical variations and cognate expressions. To put it in a simple way sign includes all kind of marks and signature is constructed by using signs or marks. Section 29A of the Negotiable Instrument Act, 1881 lays down that "no person is liable as maker, drawer, indorser or acceptor of a promissory note, bill of exchange or cheque who has not signed it as such: Provided that where a person signs any such instrument in a trade or assumed name he is liable thereon as if he had signed it in his own name."

Although the Contract Act 1872 does not specifically require every contract to be written and signed, some contracts are to be written and signed by the parties in order to be valid. For instance, Contract for sale and of sale of immovable properties. Unless a contract is properly written and signed , it is very difficult if not impossible to establish the existence of such contract and its terms and condition.

Sections 45, 47, 67 and 73 of The Evidence Act 1882 provides for the procedure to prove handwriting and signatures.[18]

3.2 Digital signature under Information Technology Act 2006

Information Technology Act of Bangladesh is an excellent effort to incorporate provisions to recognize digital signature and to lay down provisions relating implementing digital signature. The Act has tried to cover most aspects of digital signature such as public key, private key, certificate authority etc. The Act also proposes the required amendments which should be brought about in the Evidence Act in order to make digital records and signature admissible in the Court of Law.

Section 7 of the Act unequivocally recognizes digital signatures. Where any law requires authentication of a document to be made by signature, such requirement will be met by affixing digital signature to the document in the way prescribed by the law. This mean digital signature is as good as hand-writing signature provided it comply the criteria set by the Act and the document purported to be authenticated does not fall within the exceptions.

data in electronic form, 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 .

According to Section 2(1) of the Act "Digital signature" means any data in electronic form that

a) is affixed to or logically associated with a data message; and
b) the digital signature may be justified subject to the following conditions
    i) that is uniquely linked to the signatory
    ii) that is able to recognize the signatory in relation to the data message
    iii) that is created through such a secure method that can confirm the signatory's control
    iv) that is attached to the data in such a way that it can detect any subsequent alteration in the very data.

Section 5 is about authentication of electronic records by digital signature. A subscriber may authenticate an electronic record by digitally affixing digital signature by utilizing Asymmetric Cryptosystem[19] and other recognized signature making device or methods.

3.3 Certifying Authority

Certifying authorities (CA) are important entity in the Public Key Infrastructure. An example can be given to explain the role of CA. If A (the sender) and B (the receiver) are attempting to engage in an online

transaction, B needs an independent affirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that a perpetrator could have sent B the public key, contending that it belongs to A when in fact it does not. Accordingly, a reliable third party - the CA - must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[20]

3.3.1 Certifying Authorities Controller

The government may appoint Controller , Deputy Controller and Assistant Controller of Certifying Authorities. The Controller is the highest authority to supervise and validate the CAs. The Controller is responsible to specify the rules and methods under which CAs will function. It will establish databases of disclosure issued by Certifying Authorities and perform all other functions in order to ascertain the system of Public Key Infrastructure work properly.[21]The Controller has authority to recognize foreign CAs by following rules established under the Act.[22] It will act as repository of all Certificates issued.

3.3.2 License for Certifying Authorities

Certifying Authorities are generally private entities. They have to obtain license and must comply with strict requirements set by law. The Controller issues such silences after scrutinizing application for silences. The license is subject to suspension and revocation. The application should accompany a certificate practice statement, a statement including the procedures with respect to identification of the applicant, requisite fees and other documents.[23]

3.3.3 Procedures to be followed by Certifying Authority

Every CA must maintain the following standards-

a. They will make sure the hardware and software they use is safe from intrusion and misuse.
b. They will provide the reasonable level of liability in their service.
c. They will adhere to security procedures to ensure that the secrecy and privacy of the digital signature are assured.
d. They observe other standard set by rules.
e. They will make sure that every employee and otherwise engaged by it complies the rules and regulations.
f. They will disclose certain information specified in the Act.

3.3.4 Issue of Certificate

A CA will issue certificates under following circumstances.[24]

a. An application is received from an enlisted subscriber to issue a certificate.
b. The applicant is properly identified in accordance with the certificate practice statement if any.
c. The information intended to be certified is accurate.
d. The applicant holds a private key capable of creating digital signature.
e. The public key to be attached is a valid one.
f. The applicant pays requisite fees.

3.3.5 Representation

By issuing certificates the CA represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate that the Certifying authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice that contents of certificate is accurate according its practice statement. If such statement does not exist The CA represents that all the requirements of issuing certificate have been complied.[25] So it is the liability of the CA in case such requirements have not been met.

3.3.6 Revocation of certificates

CAs may revoke the certificates when the subscribers ask to do so. Death of subscriber, winding of companies, concealing of material fact, frustration of requirements, compromise of private key and insolvency may also result in the revocation of certificate.[26]

4. Evidential value of digital signature

A digital signature which is properly affixed should be evidence to the identity of the signer and content of the document signed. Despite the high level of security measures employed, digital signatures are as vulnerable as handwritten signature as far as identity theft is concerned. CAs only guarantees the authenticity of public key and they will not ensure that the private key of a person is used by that person. It is the duty and liability of a digital signature holder to keep his private key safe. In the final report of the Information Technology Bill it was proposed that amendments should be brought to the Evidence Act and Bankers Book of Evidence to facilitate presumption of evidence relating digital signature. The court shall presume the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record unless the contrary is

proved. The court shall also presume that the content of a signature certificate is authentic unless otherwise is proved.[27] However, these amendments have not been done as yet.

4. Some suggestions for effective implementation of digital signature in Bangladesh

There is much ambiguity in the Act with regard to terminology of electronic and digital signature. This is not clear what kind of signature the act recognizes. This ambiguity can be rectified through clear definitions in the Act. Countries such as Hong Kong have already amended their legislation to incorporate these definitions.[28] Enacting similar amendments will help the business community as well as other stakeholders understand what an electronic signature represents. Clarity in the legislation will enhance businesses' confidence about using the technology. In this connection the signature classification in the European E-signature Directive[29] may be followed.

Witnessing signature is another problem that has not been addressed in the Act. We know that some transaction needs witnesses to see and confirm that the intended signatory has signed the document or deal purported to be signed. To address the issue of witnessing digital signatures, a provision stating that witnessing can be done by digital signatures should be inserted into the Act. Such a provision, if included in the legislation, will eliminate the concerns of the business community, in particular, its legal advisors who believe that digital signatures and documents cannot be witnessed.

The Act does not specifically deal with the problem of admissibility of digital signature as evidence. The Evidence Act should be amended to make digital signature directly admissible and proper procedure should be incorporated in the same Act to prove digital signature in a Court of Law just like hand written signature.

It can be deduced from the Act that the law makers intended to leave certificate authorization process to the private hands. However, it will be convenient for the Government to have its own certifying authorities for sensitive documents authentication for example, national id, passports, inter department communication, military and security force and so on. This will ensure better security and efficiency in the Government works. Private Citizens can also use the service of a national Certification Authority besides the private CAs. The CA's Controller established under the Act can also act as a National CA.PKI plays a critical role in e-government by allowing governments to leverage authentication,

encryption, and digital signature technologies when issuing identity certificates, business certificates, and device certificates.[30]

Conclusion

The enactment of the Information Technology Act, 2006 and recognition of digital signature is an important building block in the legal foundation necessary for the economic development of Bangladesh and to be at par with the globalization. E- Commerce offers tremendous business opportunities for Bangladesh and the Information Technology Act has the potential to act as facilitator to take advantage of those opportunities although the Act has been criticized to be loosely based on the Indian similar Act. However, it is sadly noted that the Act has not been implemented and operational by the Government till now. The cause of which may be identified as the lack of awareness and lags in policy decision. It is expected that the government will soon take steps to implement the Act with necessary amendments.

Work Cited:

---

1 Srivastava, Aashish, *Legal Understanding and Issues with digital signatures- An Empirical Study on Large Business*, 35 Rutgers Computer & Technology and Law Journal. 42, 2008 p. 1.

2 Model Law on Electronic Signatures with Guide to Enactment at 1, U.N. Sales No. E.02.V.8 (2001), available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

3 http://www.w3.org/Signature/Activity.html last visited on January 21, 2010.

4 Stephen E. Blythe, *Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce with Secure Cyber-Transactions,* 17 Transnational Law & Contemporary Problems 361, Spring 2008, p2.

5 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html last visited on January 22, 2010.

6 Ford, Warwick, *Computer Communications Security, Principles, Stand Protocols and Techniques*, Prentice Hall, Englewood Cliffs, NJ, 1994, page 109

7 According to Section 2 (zf) of Information Technology Act 2006 , "public key" means the key of a key pair used to verify a digital signature and listed in a Digital Signature Certificate.

8 Fillingham, David**,** *A Comparison of Digital and Handwritten Signatures,* Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997,p 3.

9 Legal Implications of E-commerce: Basic Issues, Initiative and experience in Asia, United Nation's *Trade and Investment Division, Staff Working Paper 02/07, page 4.*

[10] Neumann, Peter G., *Computer Related Risks*, Addison-Wesley Publishing Company, 1995, page 170.

[11] Supra not 8 at p 3.

[12] "Private key" means the key of a key pair used to create a digital signature.

[13] Laurie, Ben Bohm , Nicholas, *Signatures: an Interface between Law and Technology*, 2003 retrieved from http://www.apache-ssl.org/tech-legal.pdf last visited on January 23, 2010.

[14] Supra note 4 at p 4.

[15] The main idea of the figure is taken from the lecture slides of **Anna Nordén,** Guest Lecturer, Master of Law and Information Technology, Stockholm University.

[16] Hossain, Najmul, *E-Commerce in Bangladesh: Status, Potential and Constraints, JOBS Report, 2000, p 2, retrieved from* http://www.jobsproject.org/content/publication/E-Commerce_in_Bangladesh_status.pdf last visited on January 27, 2010.

[17] Final Report on The Law on Information Technology, Bangladesh Law Commission, P 3, retrieved from http://www.lawcommissionbangladesh.org/wplit.html.

[18] *Abdul Gani Malitha Vs. Sariatullah Biswas ,16 DLR 157*

[19] "Asymmetric cryptosystem" means a system capable of generating a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

[20] Supra note 4 at p 6.

[21] Section 18 and 19 of Information Technology Law , 2006.

[22] Id. Section 20.

[23] Id. Sections 22 to 26.

[24] Id. Section 36.

[25] Id. Section 37.

[26] Id. Section 38.

[27] Second Schedule in the final report on the of Information Technology Bill , proposed amendments to Evidence Act, 1872.

[28] Electronic Transactions (Amendment) Ordinance, No. 14, (2004) O.H.K. §§2, 29, 30.

[29] Directive 1999/93/EC

[30] National PKI: The Foundation of Trust in Government Programs, Verisign White Paper , retrieved from www.verisign.com , p 4.