

SECOND CHAPTER

Digital signature and electronic record

5. Authentication of electronic records by digital signature.- (1) Subject to the provisions of section 2 of the Act, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric cryptosystem or recognized signature making machine or method.

6. Legal recognition of electronic records.- Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form:

Provided that information or any matter shall be accessible so as to be usable for a subsequent reference.

7. Legal recognition of digital signatures.- Where any law provides that-

(1) Information or any matter shall be authenticated by affixing the signature; or

(2) Any document shall be signed or bear the signature of any person;

Then, notwithstanding anything contain in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

8. Use of electronic records and digital signatures in Government office etc.- (1) Where any law requires,-

(a) The filing of any form, application or any other document with any office, body, authority or agency owned or controlled by the Government in a particular manner;

(b) The issue or grant of any license, permit, sanction, approval or order by whatever name called in a particular manner;

(c) The receipt or payment of money in a particular manner,

Then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case

may be, is affected by means of such electronic form as may be prescribed by the Government.

(2) The Government may, for the purposes of sub-section (1) of this section, by rules, prescribe the manner and format in which such electronic records shall be filed, created or issued, the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record.

9. Retention of electronic records.- (1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:-

(a) The information contained therein remains accessible so as to be usable for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

(3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records.

10. Electronic Gazette.- Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette:

Provided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

11. No liability to accept documents in electronic form.- Nothing contained in this Act shall confer a right upon any person to insist that any Ministry or Department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

12. Power to make rules by Government in respect of digital signatures.- The Government may, for the purposes of this Act, by rules, prescribe in the electronic Gazette or official Gazette:

- (a) The type of digital signature;
- (b) The manner and format in which the digital signature shall be affixed;
- (c) The manner or procedure which facilitates identification of the person affixing the digital signature;
- (d) The control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
- (e) Any other matter which is necessary to give legal effect to digital signatures.

Discussions

DEFINITION OF DIGITAL SIGNATURE

The digital signature is an encrypted digest of the file (message, document, driver, program) being signed.¹ And a "Digital signature" is impossible to forge. Instead, the digital signature comes from a digest of the text encrypted and sent with the text message. The recipient decrypts the signature and retrieves the digest from the received text. A match authenticates the message.² Digital signatures are required for open systems and need higher security levels.³ An electronic signature that authenticates the identity of the sender, ensures the original content of the message is unchanged, is easily

1 http://www.pcmag.com/encyclopedia_term/0,2542,t=digital+signature&i=41384,00.asp

2 <http://www.ecxweb.com/glossary.html>

3 Glossary of terms, Pharmaceutical Technology, Jun 1, 2005.

<http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=166375>

transportable, cannot be easily repudiated, cannot be imitated, and can be automatically time-stamped.¹ Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. An electronic signature is "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." They are the electronic equivalent to handwritten signatures on paper and may be based on biometric identification methods or facial and voice recognition. A simple combination of a user ID and password also is sufficient. Within a company, the user ID must be unique to a specific person.²

The Section 2(1) of the ICT Act, 2006 defines the "Digital signature" as "In this Act, unless the context otherwise requires- (1) "Digital signature" means any data in electronic form that (a) is attached with some other electronic data reasonably; and (b) Any justification of any digital signature will be done subject to the following conditions- (i) That is attached with the signer similarly; (ii) That is able to recognize the signer; (iii) That is created through such a secure method that can confirm the signer's control; and (iv) That is attached to the data in such a way that it can recognize any change in the very data.

The ICT Act allows a person to satisfy a legal requirement for a manual signature by using an electronic communication that contains a method that identifies the person and indicates their approval of the information communicated. The method by which a person is identified electronically is commonly called an "electronic signature", however the choice of a particular method must be as reliable as appropriate in the circumstances. The legislation provides flexibility for people and businesses to determine the signature technology that is appropriate to their particular needs. The method need not be a unique identifier.

Therefore, a digital signature is an electronic signature based on cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the

1 <http://www.techarch.state.ar.us/domains/security/overview/glossary.htm>

2 Glossary of terms, Pharmaceutical Technology, Jun 1, 2005.
<http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=166375>

signer and the integrity of the data can be verified.¹ Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security.² Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be.³

MEANING OF ELECTRONIC RECORDS

Electronic records are records communicated and maintained by means of electronic equipment. Electronic records are "any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."⁴ Electronic Records created by means of a computing device and subsequently stored on an electronic storage media and only retrievable through electronic means.⁵

According to section 2(7) of the ICT Act, 2006, "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche. For purposes of this definition, "electronic records" does not include or refer to photocopies, digital imaging systems, or analog or digital audio and video tapes.⁶

LEGAL RECOGNITION OF ELECTRONIC SIGNATURES & ELECTRONIC RECORDS

In some countries, including the United States, and in the European Union, electronic signatures and electronic records have legal significance. However, laws concerning electronic signatures do not always make clear their applicability towards cryptographic

-
- 1 Glossary of terms, Pharmaceutical Technology, Jun 1, 2005.
<http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=166375>
 - 2 http://www.webopedia.com/TERM/d/digital_signature.htm
 - 3 http://www.webopedia.com/TERM/d/digital_signature.htm
 - 4 Glossary of terms, Pharmaceutical Technology, Jun 1, 2005.
<http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=166375>
 - 5 Oregon State University, *Archives & Records Management Handbook*, Archives and Records Management Program.
<http://osulibrary.oregonstate.edu/archives/handbook/definitions/>
 - 6 Oregon State University, *Archives & Records Management Handbook*, Archives and Records Management Program.
<http://osulibrary.oregonstate.edu/archives/handbook/definitions/>

digital signatures, leaving their legal importance somewhat unspecified. "ICT Act 2006 has attempted to bring about electronic governance by giving legal recognition to electronic records and digital signatures and using them in government and its agencies. It has drawn parallelism in electronic information and paper and ink based information and also has given legal force or backing to treat electronic signatures at par with paper and ink-based signatures. In order to know with whom one is doing business on the web, in order to bring non-repudiation, authenticity in transactions on the Internet and pinpoint the originator of information, the IT Act provides for the deployment of digital signatures. This would allow for and encourage individuals and organizations to shop and do business and thus tap greater commerce potential via the medium of the web."¹

Section 7 of the ICT Act, 2006 gives legal recognition to digital signatures. Digital signatures have been legalised in Bangladesh since 2006. However, since then, hardly any provisions of the Act have been implemented. Section 7 of the ICT Act, 2006 gives legal recognition of digital signatures as -

Where any law provides that

- (1) Information or any matter shall be authenticated by affixing the signature; or
- (2) Any document shall be signed or bear the signature of any person;

Then, notwithstanding anything contain in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Government.

The ICT Act which provides legal recognition to Digital Signatures on par with hand-written signatures, defines the legal and administrative framework for the establishment of a Public Key Infrastructure in the country.

Section 6 of the ICT Act, 2006 gives legal recognition to electronic records. electronic records have been legalised in Bangladesh since 2006. However, since then, hardly any provisions of the Act have been implemented. Section 6 of the ICT Act, 2006 gives legal recognition of electronic records as -

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then

1 NIC Certifying Authority (NICCA). <http://nicca.nic.in/>

A Text Book on Cyber Law in Bangladesh

notwithstanding any contain in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form:

Provided that information or any matter shall be accessible so as to be usable for a subsequent reference.

The ICT Act sets out the fundamental principle that an electronic record is not subject to legal challenge merely because it is in electronic form. It provides that a legal requirement for writing is satisfied by an electronic record if the record is accessible and capable of retention for subsequent reference. If information is required by law to be delivered or sent to a person it may be delivered or sent by electronic means. It also provides that, where a signature is required by law, an electronic record meets that requirement if the method of identifying the signatory meets certain requirements. The minimum requirements for an electronic record are to be regarded as the functional equivalent of an original. It is provided that the requirements for the storage of documents, information or records in electronic form. An electronic record will not be denied admissibility in evidence solely on the ground that it is in electronic form or that, if it is the best evidence, on the ground that it is not in the original form.

Although statutory recognition is attached to the digital signature, their legal status is yet to be well-defined and interpreted since the validity of digital signatures has not yet been challenged in any Bangladeshi court.

However, ICT Act, 2000 and the amendments made in the Evidence Act consequent to the passage of ITA-2000 provide a legal recognition for any electronic document in any offence that falls under the Penal Code or any other Act in Bangladesh. Hence e-mails, Web pages, chat room transcriptions, message boards are all equivalent to print publications for the purpose of determining defamation, obscenity etc. A publisher is therefore liable for every such content if the evidence is properly presented in a court of law.

CATEGORIES OF DIGITAL SIGNATURES¹

Digital Signatures may be categorised into three classes. Class one defines the certificates that do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.

¹ Ketan Parekh, Digital signatures in India, Network Magazine, October 2006. <http://www.networkmagazineindia.com/200610/coverstory03.shtml>

The class two category states that a person's identity is to be verified against a trusted, pre-verified database. Class three requires the person present himself or herself in front of a Registration Authority (RA) and prove his/her identity.

The digital certificate usually contains data such as the owner's name, company and address, as well as the owner's public key, along with the certificate's serial number and validity period. The certificate also includes the certifying company's ID and its digital signature.

The credit investigation, loan processing, underwriting and document preparation steps can also be done electronically. The borrowers can sign all the loan papers, and the mortgage or trust deed can be notarised over the Internet. Funds can be wire-transferred along with electronic authorisation.

METHODS OF THE AUTHENTICATION OF ELECTRONIC RECORDS BY DIGITAL SIGNATURE

Section 5 of the ICT Act, 2006 states about the methods of the authentication of electronic records by digital signature. There are following methods of authentication of electronic records by digital signature.

- (i) According to section 5(1) of the ICT Act, 2006, any subscriber may authenticate an electronic record by affixing his digital signature;
- (ii) According to section 5(2) of the ICT Act, 2006, the authentication of the electronic record shall be effected by the use of asymmetric cryptosystem or recognized signature making machine or method.

A method for verifying the source of an electronic document located on a computer network, wherein said electronic document is viewed through a Document Viewer, which includes incorporating a document identifier into the electronic document. The document identifier contains identifying information related to the electronic document. These records are compared with the verification signal, and a reply signal is generated, which is transmitted back to the Document Viewer. If the information in the verification signal does not match the information contained in the information and location records, then an error message may also be generated, which is sent to a designated recipient as notification of the error.¹

¹ The Microsoft Press, Computer Dictionary, 3rd edition, 1997, p. 512. Cotter and Messing, "Electronic Filing in the Pima County Small Claims Court—Technical Parameters, Adopted Solutions, and some of the Legal Issues Involved", 38 Jurimetrics J. 397-406

USE OF ELECTRONIC RECORDS AND DIGITAL SIGNATURES IN GOVERNMENT OFFICE

Electronic records and digital signatures may be used in Government office under section 8 of the ICT Act, 2006 in following cases:

- (a) Where any law requires, the filing of any form, application or any other document with any office, body, authority or agency owned or controlled by the Government in a particular manner;
- (b) Where any law requires, the issue or grant of any license, permit, sanction, approval or order by whatever name called in a particular manner; and
- (c) Where any law requires, the receipt or payment of money in a particular manner.

Then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is affected by means of such electronic form as may be prescribed by the Government.

Therefore, the Government may, for the purposes of this section, by rules, prescribe the manner and format in which such electronic records shall be filed, created or issued, the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record.¹

RETENTION OF ELECTRONIC RECORDS

Electronic records retention is the Act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy. To expand on this definition, an electronic records retention program is that component of an organization's larger records management program that provides policies and procedures specifying the length of time that computer-based records must be maintained. Section 9 of the ICT Act, 2006 provides that

- (1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such

(Jun. 24, 1998). Newman and Smithies, "Questioned Electronic Document Examination", PenOp & American Academy of Forensic Sciences (Feb. 1997), pp. 1-8.
¹ Section 8, the ICT Act, 2006.

A Text Book on Cyber Law in Bangladesh

documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:-

(a) The information contained therein remains accessible so as to be usable for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

(3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records.

ELECTRONIC GAZETTE

Section 10 of the ICT Act, 2006 has given the recognition of Electronic Gazette as -

Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette:

Provided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

NO LIABILITY TO ACCEPT DOCUMENTS IN ELECTRONIC FORM

According to section 11 of ICT Act, 2006, nothing contained in this Act shall confer a right upon any person to insist that any Ministry or Department of the Government or any authority or body

established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

WHAT IS MEANT BY ONLINE CONTRACTS?

E-commerce portals usually specify detailed transaction rules in accordance with which any specific transaction can be initiated, conducted and concluded. A contract concluded over the Internet involves:

- The dispatch and receipt of a proposal in an "electronic record" from one contracting party i.e., the proposer/offerer, to the other party, i.e., the acceptor, and
- The acceptance of the proposal in such electronic record, by the acceptor and the dispatch of such acceptance, in an electronic record by the acceptor to the proposer.

Section 15 of the ICT Act specifies the manner and time when dispatch and receipt of an electronic record occur. Dispatch of an electronic record occurs, "when it enters a computer resource outside the control of the originator", unless agreed to the contrary between the originator and the addressee.

EVIDENTIARY VALUE OF ONLINE CONTRACTS

The ICT Act, 2006 provides for legal recognition and protection to electronic records and digital signatures. An electronic record is defined as "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche". The Evidence Act deals with the manner of providing documents by requiring proof of documents through primary evidence.

The ICT Act provides evidentiary value to electronic records by introducing an amendment of section 65 of the Evidence Act which deems any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media, to be a "document" if certain conditions specified are met.

In such cases, the information is deemed to be "admissible in any proceedings" without further proof or production of the original. Thus the electronic maintenance of records will lead to a whole scale reduction in costs in relation to record keeping as well as facilitate e-commerce