Chapter 3
[Sections: 5 to 12]
Digital signature, Electronic Signature and Electronic Records

3.1 Digital Signature vs. Electronic Signature: An analysis under this Act

1. Signature in General

In common phrasing, 'signature' means to the writing of one's name or putting a mark for authenticating or executing a document by the signatory. A signature is the name of a person or a mark or sign representing his name, marked by himself or by an authorized deputy. It is the act of signing one's name whatever the manners he uses to something. Signature whether handwritten signature or ink signature or digital signature has the following functions.

- **Evidence**: Signature is the evidence of signer[2] with the signed document.
- **Approval**: Signature expresses that the signatory[3] approves the contents of the documents by signing the document.
- **Signer Authentication**: A signature should authenticate who signs a document, record or message and should be difficult for another to produce without authorization.
- **Documents Authentication**: Signature provides what is signed so that the contents cannot be falsified without detection.[4]
- **Security:** The individuality of the style of writing or the mark grants security against forgery.
- **Binding:** A signature signifies that the parties or signatories of a document are to be bound by the signed document.[1]

---

[2] For the purpose of this Act, signer means a person who creates digital signature for message.

[3] Section 2 (35) of Information Communication Technology Act, 2006 states that "signatory" means a person providing signature generated through signature generating machine or procedure;

[4] Source: American bar Association Digital Signature Guidelines.

From the past, commercial transaction as well as any other conveyance was performed through physical signature that is said handwritten signature by the use of ink or pen. But with the growth of technology, e-commerce, and communication through internet, people use electronic records or documents instead of paper documents and now almost every business transaction and information exchange is done through online. So it can be said as online transaction or online data inter change where computer and internet are used as a media of such transaction or data exchange. The most important matter relating to online transaction is that the parties of such transaction cannot physically see each other and it may be difficult to identify whether the real person is doing the transaction or not. At the same time, in the absence of any legal binding tools, the online transaction or data interchange does not create any legal binding on the parties concern. To be sure whether the parties of online transactions are real or not, to create legal binding on the parties of such transaction, and to use such documents as evidence subsequently, it is required to use such a system by which one party of such transaction can identify the other party, can be sure that the information given by the parties are real.

So it is required to authenticate electronic record or electronic document to be sure that the information or electronic record given is original and real. We authenticate a paper document by handwritten signature but it is not possible to authenticate electronic record or data and electronic document by handwritten signature. So how can one authenticate an electronic record or document? And how can one be sure that the electronic information or electronic document is true and original? Digital signature is the answer of these questions.

Hence was born the idea of digital signatures. Though the functions and purposes of a digital signature remain the same as discussed above, the modus or the act of digitally signing e-documents is different from physical signatures on paper. The most significant difference is that the methodology used in the former is the direct performance/act of the human hand without any external dependence, whereas the latter is an external system of technology applied by the subscriber to an electronic record.[2] The concept of

---

[1] Sood. Vivek, Cyber law simplified, the tata mcgraw-hill publishing company limited, 7west patel Nagar, New Delhi 110008, 2001

[2] ibid p.436

'digital signature' which is the creation of technology has been recognized by the Information Communication Technology: 2006. The system of digital signature has been legally recognized in ICT Act:2006 with a view to facilitating e-commerce and e-governance, along with making the parties of e-transaction bound by their contractual obligations and other commitments, failing which, the aggrieved party has evidence to seek appropriate remedies under law.

2. Meaning of Digital Signature according to Section 2(1) of ICT Act, 2006

Section 2(1): in this Act, unless the context otherwise requires,

1. "digital signature" means data in an electronic form, which—

a) is related with any other electronic data directly or logically; and

b) is able to satisfy the following conditions for validating the digital signature—

(i) Affixing with the signatory uniquely;

(Ii) Capable to identify the signatory;

(iii) Created in safe manner or using a means under the sole control of the signatory; and

(iv) Related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

Comments

Information and Communication Technology Act, 2006 regards digital signature as a personalized thumbprint. There is no formal, universally accepted definition of digital signature. We are, therefore, supporting our discussion on the definition of digital signature in Information and Communication Technology Act, 2006 that has been defined digital signature in section 2(1).

According to sections 2 (1), digital signature" means data in an electronic form, which is related with any other electronic data directly or logically and is able to satisfy the conditions required for validating the digital signature. A digital signature must fulfil the following conditions to be treated as a valid Digital Signature.

(I) affixing with the signatory[3] uniquely;

---

[3] "signatory" means a person providing signature generated through

(Ii) Capable to identify the signatory;

(iii) Created in safe manner or using a means under the sole control of the signatory; and

(iv) Related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

According to section 2 sub-section 1, digital signature must be created in a safe manner or using a means under the sole control of the signatory. The manner must be safe because it enables to identify any alteration if made in the data that is sent. But what procedures will be treated as safe manner to create a digital signature has not been defined in information communication and technology act; 2006. The Information Technology (certificate authority) rules, 2010 contains the provisions relating to safe manner to create a digital signature.

A method, known as "Public Key Cryptography" (PKC), shall be used for creating and verifying electronic signature[1], the process termed as hash function shall be used in both creating and verifying a Digital Signature.[2]

3. Meaning of Electronic Signature: [Rule 2 (d) of IT (CA) Rules, 2010]

"Electronic Signature" means electronic signature as defined in section 2(1) of the Act and for the purpose of these Rules, digital signature will also be considered as electronic signature.

Comments

No definition of electronic signature has been given in Information and Communication Technology Act; 2006. In Information Technology (CA) rules; 2010, it has been said the definition of digital signature given in section 2(1) of ICT, 2006 shall also be applicable for the definition of electronic signature and for the purposes of certificate authorities rules , digital signature will also be considered as electronic signature. So the electronic signature also includes digital signature for the purposes of Information Technology (CA) rules; 2010.

---

signature generating machine or procedure;

[1] Section 3 sub-section 2, Information Technology (Certificate Authority) Rules working Draft, 2010

[2] Section 3 sub-section 3, ibid

4. Creation and verification of Digital Signature and Electronic Signature:

In e-governance[3] and e-commerce system, digital signature or electronic signature is two essential components. To use digital signature in e-governance and e-commerce, at first it must be created using safe and secure manner and subsequently must be verified to be sure that the electronic records and digital signature sent are authenticate, correct and true. The ICT Act, 2006 and IT (CA) Rules, 2010 mentioned the necessary methods by which digital or electronic signature can be created and verified. As the term 'electronic signature' also includes digital signature, so the methods of creating and verifying of electronic signature mentioned in Information Technology (CA) Rules, 2010 shall also be applicable for creating and verifying of digital signature.

(a) Creation of Electronic Signature (digital Signature) [Rules 4 of IT (CA) Rules, 2010]

To sign an electronic record or any other item of information, the signer shall apply the following methods:

(a) Use ***hash function*** in the signer's ***own software***, for all usage needs, which in the case of electronic record shall compute a ***hash result*** of standard length which is unique to the electronic record;

(b) Use ***private key*** to transform the hash result of the signer's software into an Electronic Signature;

(c) the Electronic Signature created by following the method contained in sub-Rule (a) and (b), shall be unique or uniform to both electronic record and private key used to create it; and

(d) The Electronic Signature shall be attached to the electronic record and appropriately protected and thereafter transmitted with the electronic record.

Comments

[3] The word "electronic" in the term e-Governance implies technology driven governance. E-Governance is the application of Information and Communication Technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between Government-to-Citizens (G2C), Government-to-Business(G2B),Government-to-Government(G2G) as well as back office processes and interactions within the entire government frame work.

Rule 4 of Information Technology (Certificate Authority) Rules, 2010 described the manners to create an electronic signature. As electronic signature also includes digital signature, so the method that has been described in rule 4 of IT (CA) rules, 2010 shall also be equally applicable for the creation of digital signature. Rule 4 described the methods that are used to sign an electronic record or any other electronic message and information. It states that the originator shall apply the following methods to sign an electronic record

(a) Use ***hash function*** in the signer's ***own software***, for all usage needs, which in the case of electronic record shall compute a ***hash result*** of standard length which is unique to the electronic record;

(b) Use ***private key*** to transform the hash result of the signer's software into an Electronic Signature;

(c) the Electronic Signature created by following the method contained in sub-Rule (a) and (b), shall be unique or uniform to both electronic record and private key used to create it; and

(d) The Electronic Signature shall be attached to the electronic record and appropriately protected and thereafter transmitted with the electronic record.

Beside, Rule 3 of IT (CA) rules, 2010 also contains the method of creation and verification of electronic signature. According to this rule, there are three methods described below can be used to create and verify an electronic record or electronic information.

(1) An Electronic Signature shall be created and verified by such cryptography which transform electronic records into seemingly unintelligible form and back;

(2) A method, known as "Public Key Cryptography[1]", shall be used for creating and verifying electronic signature, which employs an algorithm using two different but mathematically related "keys" – one (private key) for creating an Electronic Signature or

[1] "Public Key Cryptography" is an encryption method that uses a two-part key: a public key and a private key. To send an encrypted message to someone, you use the recipient's public key, which can be sent to you via regular e-mail or made available on any public Web site or venue. To decrypt the message, the recipient uses the private key, which he or she keeps secret. Contrast with "secret key cryptography," which uses the same key to encrypt and decrypt. The standard for public key cryptography for digital signature and digital encryption has been mentioned in schedule (2) of IT (CA) Rules, 2010.

transforming data into a seemingly unintelligible form, and another key (public key) for verifying an Electronic Signature or returning the electronic record to original form,

(3) The process termed as hash function shall be used in both creating and verifying a Digital Signature.

The American Bar association (ABA)[2] defines the term 'Digital Signature' which explains the methods of creating a digital signature. Digital signature is a transformation of a message using an ***asymmetric cryptosystem*** and a ***hash function*** such that a person having the initial message and the ***signer's public key*** can accurately determine

1. whether the transformation was created using the ***private key*** that corresponds to the signer's public key, and
2. whether the initial message has been altered since the transformation was made

Rules 4 of IT (CA), 2010 and the definition of digital signature given be American Bar Association, mentions ***asymmetric Cryptosystem, private key, public key, hash function, and hash result,*** which are used to create electronic signature or digital signature. So a digital signature is highly related with the following terms

1. ***Asymmetric Cryptosystem (ACS) consisting of private key and public key***
2. ***Hash function***
3. ***Hash result***

To create digital signature, there are two steps. They are

1. ***The use of Asymmetric cryptosystem.***
   a. **Private key (Private key is used to create Digital Signature)**
   b. **Public key (Public key is used to verify Digital Signature)**
2. ***The creation of hash result using hash function***

So for better understanding, we need to explain these terms.

I. Asymmetric cryptosystem:

Asymmetric cryptosystem is the core of digital signature technology. Asymmetric cryptosystem means a system of a secure key pairs consisting of a private key for creating a digital signature and a

[2] Digital signature guidelines by Information security committee, electronic commerce and information technology division, section of science and technology, by American Bar Association, august, 1996

public key to verify the digital signature.[1] The asymmetric cryptosystem used for creating and verifying digital signatures (but need not) include functions for encryption[2] or decrypting the message, in which case the public key of the key pairs is used for encryption and the private key is used for decryption. These two complex key pairs are created with the help of a special kind of mathematical algorithm. [3]

Private Key is the personal digits that are only available to the originator of Digital Signature. "Private Key" means secret information or electronic signature giver's known encryption or decryption key, which is used to encrypt information into electronic signature.[4] Private Key is used to originate Digital signature.

Public key is the public digits of originator of digital signature but it is open for the receivers of the electronic record or message to verify the digital signature whether it originates from the originator of digital signature. "Public key" means a specific value determined by the nominated authority, which is used as "encryption key" combining with "private key" to effectively encrypt information and electronic signature. The receiver of the electronic records or electronic messages uses public key to verify digital signature. Public key is used to verify digital signature.

ii. Hash function

An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that

1. A message yields the same hash result every time the algorithm is executed using the same message as input,
2. It is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm, and
3. It is computationally infeasible that two messages can be found that produce the same hash result using the algorithm[5].

---

[1] section 2 (f), (Indian), The Information Technology Act: 2000,

[2] In cryptography, **encryption** is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can.

[3] Ibid, section [2 (1) subsection 1 (H)]

[4] Section [2 1(G)], ibid

[5] Digital signature guidelines by Information security committee, electronic commerce and information technology division, section of science and technology, American Bar Association, august, 1996

A hash function is a math equation that creates a message digest hash result from a message. The original message or document which the digital signature is attached is converted into a comple digit. A special mathematical method is used to convert the origin message into a complex digit. The mathematical method by whic the message is converted into a complex digit is called Hash functio and the digit is called hash result.

iii. Hash result

The output produced by a hash function upon processing a message The output of a hash function is sometimes called a 'message digest'

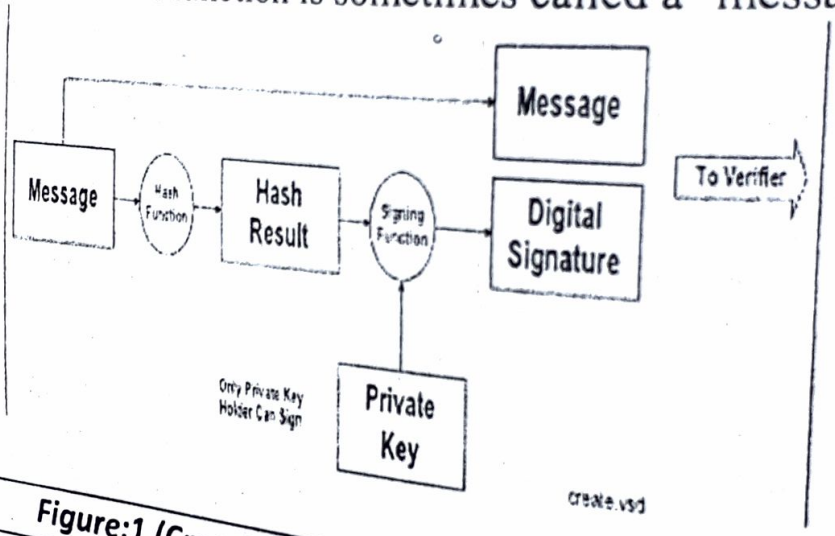

Figure:1 (Creation of Digital Signature)[7]

5. Verification of Electronic Signature (Digital Signature) [Rule 5 of IT (CA) Rules, 2010] -

(1) The verification of an Electronic Signature shall be accomplished by the following method:-

(a) By computing a new hash result of the original electronic record by means of the hash function used to create an Electronic Signature and by using the public key;

(b) The encrypted digital digest shall be decrypted by using public key;

(c) By comparing the new hash result with the decrypted hash;

(2) In instances, when:-

(a) Similar private and public key is used to create an Electronic Signature,

[6] Message means a digital representation of information.
[7] ibid

(b) Newly computed hash result is similar with the original result, and

(c) Which transforms into Electronic Signature during the signing process. The verifier shall verify the Electronic Signature.

(3) The verification software will confirm the Electronic Signature as verified if:-

(a) in order to digitally sign the electronic record, the private key of the signer is used and the public key of the signer is used to verify the signature, in that instance the electronic record shall be considered to have been digitally signed;

(b) An electronic record will be deemed to be unaltered, if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.[1]

Comments

(a) What is verification of electronic signature?

"Verification" means such procedure used to identify signatory or authentication of data message.[2] In order to digitally sign the electronic record, the private key of the signer is used to originate digital signature and the public key of the signer is used to verify the signature, in that instance the electronic record shall be considered to have been digitally signed[3]. To be secure, whether the data message[4] is authenticate or not, you must verify the digital signature as we verify handwritten signature to be sure whether the paper document on which the handwritten signature has is authenticate or not.

(b) Procedure of verification of electronic signature

At first, the receiver of electronic record shall compute a new hash result of the original electronic record by means of the hash function (own hash function software) which was used by the sender to create an Electronic Signature. Then the encrypted message digests or hash result shall be decrypted by using public key. By comparing the new hash result with the decrypted hash, if newly computed hash result is

---

[1] Rule 5, Information Technology (Certificate Authority) Rules working draft, 2010

[2] Section 2 (23), Information Communication Technology Act, 2006

[3] Information Technology (Certificate Authority) Rules, 2010, rule [5 (3)]

[4] "data message" means electronic, electronic data interchange including optical, electronic mail, telegram, telex, fax, telecopy, short message or created something similar, sent, received or stored information;

similar to the original result, then the verification software w confirm the Electronic Signature as verified and the electronic reco shall be treated as authenticate. An electronic record will be deem to be unaltered, if the hash result computed by the verifier identical to the hash result extracted from the digital signature duri the verification process.[5]

In short, it can be expounded that the digital signature is created wi the combination of both Hash function and private key. At first th sender must apply the hash function in a definite method to th document that he wants to send. A hash result will be created fo applying hash function into the document. After that the hash resul shall be converted into a unique symbol or digest that is called digita signature. All of the functions are done through compute programme. Then both the electronic document and digital signatur are sent to the receiver.

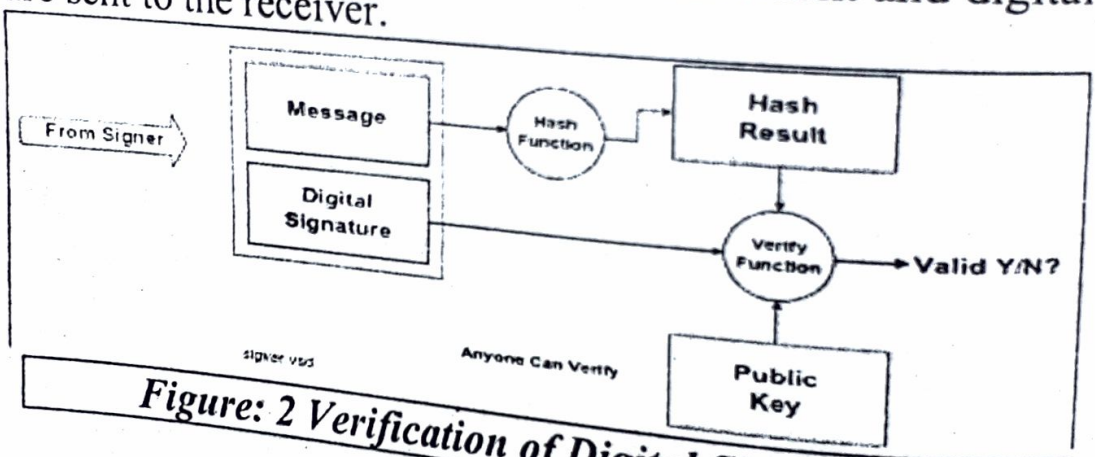

Figure: 2 Verification of Digital Signature[6]

6. Differences between digital signature and electronic signature

Signatures in the computing and internet environment may be broadly classified into following two kinds.

(1) Electronic Signature

(2) Digital signature.

This classification is according to the techniques employed in the creation, verification, and storage of the individual's identity. There is a clear difference between electronic and digital signature, though these terms are often used interchangeably and no such differences have been mentioned in ICT Act, 2006.

---

[5] Rule 5, ibid

[6] Digital signature guidelines by Information security committee, electronic commerce and information technology division, section of science and technology, American Bar Association, august, 1996

- The term electronic signature has not been defined in the ICT ACT: 2006.

It only defined digital signature. To speak generally, digital signature is a kind of electronic signature. The term electronic signature is much wider than the term digital signature. According to section 2 (d) Electronic Signature" means electronic signature as defined in section 2(1) of the Act and for the purpose of Certificate Authorities Rules; 2010, digital signature will also be considered as electronic signature.[1] In section 8 of the ICT Act: 2006, the words "electronic signature" has been used instead of digital signature. This has been done thinking that electronic signature covers the digital signature also according to section 2 (D) of Information technology (certificate Authority) rules, 2010. As electronic signature also denotes digital signature, so there is no bar to use digital signature for the purposes for which electronic signature can be used.

- A digital signature is an electronic signature, but an electronic

Signature is not necessarily a digital signature.

- A digital signature is a "secure" electronic signature which uses encryption and passwords to protect the integrity of the signature and guarantee the authenticity of the party who signed it.[2] A digital signature is generated for each message using asymmetric crypto system consisting of (private key and public key), hash function. It is not a digitalized image of a handwritten signature. Hence forgery is not possible. But electronic signatures are easy to forge.[3]

7. Legal Recognition of Digital Signature (Electronic Signature) [Section 7]

Where any law provides that--

(a) Any information or any other matter shall be authenticated by affixing the signature;

Or

---

[1] Information Technology (certificate authority) rules, 2010 section 2(d)

[2] http://searchsecurity.techtarget.com/answer/The-difference-between-electronic-and-digital-signatures

[3] *https://cdr.lib.unc.edu/indexablecontent?id=uuid...3a7f..*

(b) Any document shall be authenticated by signature or bear the signature of any person;

then, notwithstanding anything contained in such law, such information or matter is authenticated by means of digital signature affixed in defined manner or so is the case of any document.

Comments

Has there any recognition of Digital Signature in Bangladesh?

Digital signature has been given recognition in section 7 in ICT Act, 2006. Section 7 of ICT Act and section 2 (d) of IT (CA), Rules recognizes the legal validity of both digital signature and electronic signature for the purposes of electronic records, e-commerce and e-business and e-governance. This legal recognition of digital signature and electronic signature was required as numerous individuals, companies, firms and various other kinds of businesses and social organizations have been continuing their social, business and other commercial transactions through digital signature. It has been said that where any law provides that--

a) Any information or any other matter shall be authenticated by affixing the signature; Or

b) Any document shall be authenticated by signature or bear the signature of any person; then, notwithstanding anything contained in such law, such information or matter is authenticated by means of digital signature affixed in defined manner or so is the case of any document.[4]

8. The usages of digital signature and electronic signature

Now the question is what will be if digital signature or electronic signature is introduced. The primary discussion of digital signature and electronic signature clarifies that in the era of e-governance, e-commerce, the introduction of digital signature is a must. The main purposes of enacting of this Act are to introduce e-governance, e-commerce, and e-contract. These shall not be secure and successful unless and until digital signature and electronic signature are recognized in legal system. To this end, digital signature and electronic signature have been recognized in section 7 of ICT Act, 2006. ***[To know details about e-governance and e-commerce, please see chapter 20 and 21]***

[4] Section 7, ibid

The usages of electronic signature and digital signature are mentioned below.

(a) Use of **digital signature to authenticate electronic records (Section 5)**

(1) Subject to the provision of sub-section (2) of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of electronic record shall be effected by the use of technology neutral system or standard authentic signature generating machine or strategy.

Comments

According to section 5 of ICT Act, 2006, any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of electronic record shall be effected by the use of technology neutral system or standard authentic **signature generating machine**[1] or strategy. In other words, hand written signature is used to authenticate paper document where digital signature or electronic signature is used to authenticate electronic records. ***(For further information, please see :)***

(b) Use of Electronic Signature in Government offices and its agencies [Section 8]

According to section 8 of ICT Act, 2006 Electronic signature can be used in Government and its agencies for

(1) The filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner. So, for this section, electronic signature

(2) the issue or grant of any licence, permit, sanction, approval or order by whatever name called in a particular manner;

(3) the receipt or payment of money in a particular manner;

(4) then, notwithstanding anything contained in such law, filing, issue, grant of the document and

[1] signature generating machine" means software or hardware used generating data for creating signature; Section 2(37)

(5) Receipt and payment of money, as the case may be, is affected by means of prescribed electronic form.

Comments

Section 8 is the most important section which is essential to introduce e-governance[2] in Bangladesh. For this section, e-governance as well as e-commerce has got a legal recognition.

1) To run E-procurement
2) To run e-commerce, e-transaction in Bangladesh
3) To be possible to do online transaction safely
4) To submit income tax return as well as other fees through online
5) One will be able to buy trough online.
6) Tender Bazi will be stopped
7) To submit any online application for any kinds of citizen's service. So it will not be necessary to go to the office to submit application.
8) To ensure secured Socket Lair (SSL)[3] based security in the web server, e-mail server as well as other server
9) To communicate digitally among various departments of government. It will create inter ministerial communication that will enhance the quality and speed of government's activities
10) To run paperless office and e-failing. it will reduce the use of huge paper in the departmental activities of government and non government institutions
11) There will be no possibility to disclose the confidential information of government and it will protect the privacy of the government
12) To sign electronic document, e-mail, and electronic records. So the parties of online transaction or online information

---

[2] Electronic governance is a government run through the use of information and communication technology that serves a variety of different ends: better delivery of government services to citizens, improved interaction with business and industry, citizen empowerment through access to information, or more efficient government management. **(for further reading, see chapter 19)**

[3] The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.

exchange are able to identify the identity of the person, the authenticity of the information submitted.

13) To enable to investigate any kinds of cyber crimes

3.2 Electronic Records

1. What is electronic record?

Section 2 (7) describes "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. Under this subsection 'electronic record' includes

1) Data
2) Record or data generated
3) Image or sound stored
4) Received or sent in an electronic form
5) Microfilm or computer generated microfiche

Illustration

An email, picture, image or sound, fax message generated using computer, contents of a website etc. Banglalink sent you a 'SMS' that you have a special 100% bonus offer if you costs double amount than that you did in the previous month. This 'SMS' is an electronic record as it is sent in an electronic form.

2. Authentication of electronic records by digital signature [Section 5]

1) Subject to the provision of sub-section (2) of this section, any subscriber may authenticate an electronic record by affixing his digital signature.
2) The authentication of electronic record shall be effected by the use of technology neutral system or standard authentic signature generating machine or strategy.

Comments

What does authentication of electronic records by digital signature mean?

The most important use of digital signature is the authentication of electronic records by it. Electronic records in the electronic communication system such as communication through internet or sending e-mail using internet cannot be believed until and unless there is a strong basis of believing it. Authentication of

electronic record by affixing digital signature is the strong basis that creates a reasonable ground in the mind of a man to believe that the message has been originated and sent from proper sources.
Authentication is a process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transmission.
How electronic record can be authenticated has been discussed in section 5 of ICT Act; 2006 that states that a subscriber may authenticate an electronic record by affixing his digital *signature*. But what will be the moods of authentication to effect electronic record has been discussed in section 5 (2). The authentication of electronic record shall be effected by the use of ***technology neutral system or standard authentic generating machine*** or strategy. Here the term "standard authentic generating machine" means software or hardware used to generate data for creating signature.[1]

3. Legal recognition of electronic records (section 6)
Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such information or matter is rendered or made available in an electronic form:
Provided that such information or matter is accessible so as to be usable for a subsequent reference

Comments

Has there any Legal recognition of electronic records
Electronic records have been recognized in section 6 of ICT Act, 2006. This section contains that "Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such information or matter is rendered or made available in an electronic form. Provided that such information or matter is accessible so as to be usable for a subsequent reference.[2]

Illustration
The submission of application through SMS from Teletalk for admission test of public university and submission of online job

[1] Section 2 (37), ibid
[2] Section 6, ibid

application are the instances of electronic records as these applications are generated electronically and stored in an electronic form. When anyone saves or receives those sms or applications in mobile or computer hard disk, then such storing, saving or receiving in an electronic form. These electronic records have been legally recognized and can be used for subsequent reference.

4. **Retention of electronic records. (Section 9)**

1) Where any law provides that any document, record 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 a 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 sub-clause does not apply to any information which is automatically generated solely for the purpose of enabling and 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 that expressly provides for the retention of documents, records or information.

Comments

What are the needs of retention of electronic record?

Electronic records have same evidentiary value like paper documents because section 87 of Information and Communication Technology

Act, 2006 states that the definition of "document" in section 29 of Penal Code, 1860, the definition of "document" in section 3 of Evidence Act, 1872, also include the documents generated or prepared by electronic machine or technology. On the other hand, the definition of "bankers books" in section 2, Clause (3) of Banker's Books Evidence Act, 1891 also includes the books viz. ledgers, day-books, cash-books, account-books and all other books generated or prepared by electronic machine or technology;

So an electronic record can be used as evidence and as such it may be required to retention of electronic records for subsequent reference. So retention of electronic records may be interpreted as requiring the retention of paper documents. That means electronic records should retained for the same purposes for which we retain the paper documents.

Conditions of retention of electronic records:

Section 9 prescribes that an electronic record shall be retained where any law provides that any document, record or information shall be retained for any specific period. An electronic record shall be deemed to have been retained if such electronic records or information are retained in an electronic form if the following conditions are satisfied-

a) the information contained therein remains accessible so as to be usable for a 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 it can be demonstrated to represent accurately the information originally generated, sent or received;

c) such information enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received,

Provided that the provisions of these sub-clauses (a, b, and c) do not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Sub section 3 of section also mentions that nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information.

3.3 Electronic gazette (Section 10)

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 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.

Comments

What is Electronic Gazette?

"Electronic gazette" means the official gazette published in the electronic form in addition to official printed & published gazette. To ensure the right to information for the citizens of a country, it is required to publish government's notification in an electronic gazette along with paper based gazette. For this provision, any laws, rules, regulations and notifications can be published in electronic gazette along with official gazette. Sections 10 states that 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 Electronic Gazette. 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.

For example, when the 7th Bangladesh Judicial Service Commission (BJSC) preliminary exam result was published, at first it was published in official gazette of BJSC's office and subsequently, the result was also published in an electronic gazette to its website named www.bjsc.gov.bd.

This section really facilitates the electronic governance in our country. Now in Bangladesh, every ministry of government publishes its notification, rules, and laws in electronic gazette to its own website. The laws of our country are available at

www.bdlaws.minlaws.gov.bd. Any job circular of Bangladesh Public Service Commission (BPSC) is published in electronic gazette to its website at www.bpsc.gov.bd. This ensures the right to information of people.

3.4 No liability on Government to accept documents in electronic form (Section 11)

Nothing contained in this Act shall by itself compel 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.

Comments

Can the Government be compelled to accept documents in electronic forms?

Section 11 of ICT Act, gives the Government exemption from being compelled to accept documents in electronic form. According to this section, the following Government authorities cannot be compelled to accept issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

(a) Any ministry or department of the Government

(b) Any authority or body established by or under any law or controlled or funded by the Government

So it is the discretion of the Government authorities whether they will accept any documents in electronic form or not. This section is a hindrance to run electronic governance and electronic commerce in Bangladesh because no liability shall be imposed upon the Government and its agencies if it/ they don't accept documents in electronic form.

3.5 Power of Government to make rules in respect of digital signatures?—

The Government may, by notification in the Official Gazette and in additionally optionally in the Electronic Gazette, make the following rules (all or any of them) to prescribe for the purposes of this Act--

(a) The type of digital signature;

(b) The manner and format in which the digital signature shall be affixed;

(c) The manner and 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 and payments; and

(e) Any other matter which is necessary to give legal effect to digital signatures