International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 27-07-2020; Accepted: 12-08-2020; Published: 29-08-2020
www.lawjournals.org
Volume 6; Issue 4; 2020; Page No 294-296

Digital signature-the electronic fingerprints

Rutveek Jawalekar
Saurabh, Ramdaspeth, Arvind Gosh Marg, Akola, Maharashtra, India

Abstract
The speedy development of electronics & communication technologies over a couple of decades has revolutionized both business and individual practices. The worldwide outburst of electronic commerce and the developments in the computer and telecommunication sector are swiftly changing the availability of information and services. Various documents are authenticated electronically. Similarly, digital evidence has transformed itself as a magical window that could see the past and in the mind of the criminal through the recovery of the electronic data. This article summarizes the concept of Digital Signature, digital evidence its relevance, admissibility and types.

Keywords: digital evidence, digital signature, digital certificate, information technology

Introduction

Around twenty years ago, a technocrat minister with a black briefcase climbed the steps of the of the Parliament to enter the cold, thick-walled room of the Lok Sabha with a happy and smiling gesture. Late Mr. Pramod Mahajan had a mission on that day the Parliament had never heard of, which eventually became one of the most revolutionary legislation named as The Information Technology Act, 2000.

The briefcase he carried contained the proposed bill that would provide a legal framework for electronic governance by recognizing digital signatures and electronic records. It also defined and recognized cyber space and prescribed penalties for its misuse. The Parliament enacted the bill and the hon'ble President K. gave his assent on 9th May 2000 making India the 12th country to enable the cyber law.

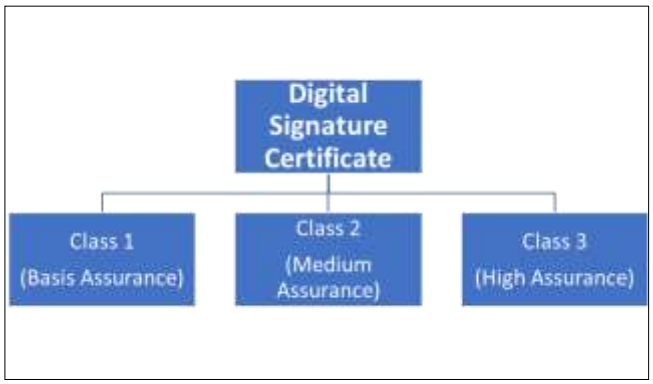
The Act which commenced on October 7th, 2000 proved to be extraordinary as it provided legal recognition for transactions which involved the use of alternatives to paper-based methods of communication. Further, the Act also went on to amend The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891and matters connected therewith which marked the beginning of e-commerce in the country.

- **Digital Signature**

Digital Signature is everything about using a mathematic function and using it to validate the authenticity and integrity of a document or a message. It can be used for a software or a digital-based document and are more competent with its confidential handling of every data. With digital signature, there is enhanced security as well as integrity that helps in preventing security problems like impersonation and tampering with digital documents.

- **Types of Digital Signature Certificate (DSC) [1]**

The Digital Signature Certificates can be classified into three categories.



- **What is DSC?**

Digital Signature Certificate is an electronic mark to sign records for the approval purposes like the typical reports approved by written by hand signature and manual confirmation.

- DSC are often required for a few applications, for instance, GST, e offering, EPFO, PF, NRI, MCA21 e-recording then forth.
- DSC kinds of Class I, Class II, Class III are accessible. DSC are often connected by Individuals, Organizations. Legitimacy of the DSC are going to be 1 year or 2 years.
- Principle superiority of getting dsc testament is to diminish your expense and time, your report legitimacy is verified.
- Reports which are marked cannot be altered or adjusted again in future so on guard the records.

- **Class 1 (Basis Assurance)**

This provides a basic level of assurance relevant to environments where there are risks and consequences of knowledge compromise, but they're not considered to be of major significance.

- **Class 2 (Medium Assurance)**

This level has relevancy to environments where risks and consequences of knowledge compromise are moderate. this

[1] Emudhra.

might include transactions having substantial price or risk of fraud, or involving access to non-public information where the likelihood of malicious access is substantial.

- **Class 3 (High Assurance)**

This level has relevancy to environments where threats to data are high or the results of the failure of security services are high. this might include very high value transactions or high levels of fraud risk.

- **Conditions for the admissibility of digital evidence [2]**

Before a computer output is admissible conspicuous, following conditions must be fulfilled, as began in section 64(B)(2):

• The conditions mentioned in sub-section (1) in respect of a computer output shall be the subsequent, namely: -

(a) the pc output containing the knowledge was produced by the pc during the amount over which the pc was used regularly to store or process information for the needs of any activities regularly carried on over that period by the person having lawful control over the utilization of the computer;

(b) during the said period, information of the type contained within the electronic record or of the type from which the knowledge so contained springs was regularly fed into the pc within the ordinary course of the said activities;

(c) throughout the fabric a part of the said period, the pc was operating properly or, if not, then in respect of any period during which it had been not operating properly or was out of operation during that a part of the amount, wasn't like to affect the electronic record or the accuracy of its contents; and

(d) the knowledge contained within the electronic record reproduces or springs from such information fed into the pc within the ordinary course of the said activities.

• Where over any period, the function of storing or processing information for the needs of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether-

(a) by a mixture of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in the other manner involving the successive operation over that period, in whatever order, of 1 or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the needs of this section as constituting one computer;

- **Where are electronic signatures not valid?**

Not all documents having electronic signatures are valid or legally enforceable. Few of the subsequent documents can't be digitally signed.

- Negotiable instruments like a note or a bill of exchange aside from a cheque
- Powers of attorney
- Trust deeds
- Wills and the other testamentary disposition
- Real estate contracts like leases or sale agreements

The above documents must be executed using traditional "wet" signatures so as to be legally enforceable.

- Admissibility of E- agreements as evidence?

Section 47A of the Evidence Act stipulates that when the Court has got to form an opinion on the electronic signature of a person, the opinion of the Certifying Authority which has issued the electronic Signature Certificate may be a relevant fact, and Section 85B of the Evidence Act stipulates that unless the contrary is proved, the Court shall presume that-

- the secure electronic record has not been altered since the precise point of your time to which the secure status relates;
- the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record.

- **Steps to Apply for a Digital Signature Certificate [3]**

1. Log on to a Certifying Authority licensed website that issues Digital Certificates in India and select your type of entity.
2. Fill in the necessary details after downloading the DSC application form. After filling all the compulsory details attach your recent photograph and mark your signature under the declaration. Check from top to bottom whether the form is completely filled or not. Print the completed form and safeguard it.
3. The assisting documents such as identity and address proof must receive attestation by an attesting officer.
4. To get digital signature online, one must get a demand draft or cheque for the payment of application form in the Local Registration Authority's name.
5. After enclosing the following mentioned documents in an envelope, post them.

1. Duly completed DSC registration form
2. Identity and address proof documents attested by the attesting officer.
3. Demand Draft or Cheque for payment of form.
4. Mark the enclosed envelope addressing to the Local Registration Authority (LRA) and post the enclosed envelope to the referred address of the LRA for further processing of the shape.

After completing the above-mentioned steps i.e. after filling the DSC Form and providing all the specified documents and payment, application process of Digital Signature Certificate is completed successfully.

Conclusion

The electronic medium of authentication may be a fairly new concept. Digitization has helped achieve tremendous results. it's also saved tons of your time and paperwork. Moreover, it's given simple accessibility.

But the law regarding the admissibility of digital evidence has got to go an extended way. Presently, the admissibility of digital information as evidence has got to be judged within sections of 65B of the Evidence Act and if the evidence is without a certificate u/s 65B, it's not admissible. there's a robust sense of confidence among activists that the Indian Judiciary will take necessary steps

[2] Digital Evidence and Electronic Signature Law Review, Vol 5, By Tejas D. Karia

[3] https://www.vsign.in/blog/different-types-of-digital-signature-certificate-and-their-use

regarding digital evidence because it has proved in history multiple times.

- **Frequently Asked Questions**

Q: Is a digital signature legally valid?
A: Yes, the Information Technology Act, 2000 in India has given legal validity to digital signatures.
Q: Can two or more people have the same digital signature?
A: No, a digital signature is unique and thus two or more individuals/entities cannot have the same digital signature.
Q: What is the validity of the digital signature?
A: You can choose to obtain a digital signature of 1 year or 2-year validity from date of issuance.
Q. Can a person have two digital signatures say one for official use and other one for personal use?
A: Yes, a person can have two Digital Signature Certificates (DSC) and it depends on him which he wants to use for personal purpose and which for official purpose.
Q: What is the difference between a Digital Signature and a Digital Signature Certificate?
A: A digital signature is an electronic method of signing an electronic document whereas a Digital Signature Certificate is a computer-based record that

- Identifies the Certifying Authority issuing it.
- Has the name and other details that can identify the subscriber.
- Contains the subscriber's public key.
- Is digitally signed by the Certifying Authority issuing it.
- Is valid for either one year or two years.

References

1. https://www.e-mudhra.com/faq.html
2. https://blog.ipleaders.in/e-signature-bane-or-boon/#Landmark_Cases
3. https://www.e-mudhra.com/Class-of-certificates.html
4. http://www.mca.gov.in/MinistryV2/digitalsignaturecertificate.html
5. https://www.quora.com/What-are-the-types-and-usages-of-the-digital-signature-certificate-DSC
6. https://www.vsign.in/blog/different-types-of-digital-signature-certificate-and-their-use
7. http://vinodkothari.com/2019/10/validity-of-e-agreement-and-e-signature/