INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

DIGITAL SIGNATURE UNDER THE INFORMATION TECHNOLOGY ACT 2000, WITHIN THE SPHERE OF THE INFORMATION TECHNOLOGY LAW - AN APPRAISAL OF ITS LEGALITIES

AUTHORED BY - STUTI SHARMA
(BBA LLB, LLM, PhD)

ABSTRACT

ensures that the communication has not been tampered and confirms the creator's independence. A hash task produces a hash value which is also known as significance digest. It plays a vital role in ensuring that the message has not been tampered and in sequence and is safe and secure.

RESEARCH OBJECTIVES

- To understand the technicality of the digital signature and its legal effect.
- To study the effect, scope and nature of digital signature.
- To study the impact of the digital signature under section 2, 3 and 15 of the Information Technology Act, 2000.

RESEARCH METHODOLOGY

In this research project, I have included doctrinal way of research. Descriptive technique will be used to value the meaning, scope and importance of the digital signature. Analytical way will be included to classify various judgments connecting to digital signature usage in Indian Legal system to get an insight of its permissibility in the Indian courts and its vital aspect for creating secure environment for electronic transactions and to achieve its objectives.

RESEARCH QUESTION

- Whether the analysis show that 'digital signature' under the Information Technology Act, 2000, is one of the crucial aspect for creating safe environment for electronic transactions and creates a sense of authentication and non-repudiation and therefore ultimately achieve its objectives of facilitating e-commerce?

ISSN: 2582-6433

LITERATURE REVIEW

A considerable amount of research has been done on effect of digital signature procedure under the information technology act. The literature is obtained in the form of reports and research studies, is briefly reviewed in this part.

- **Hanscom CB, journal of Information Technology, 2010[1]** -In this research article, the author has done concentrated research on the impact of the digital signature. It helped me to get through the basics of digital signature and why it was introduced.
- **Dr. Dharmendra Kumar Singh, Constitutionality and evidentiary value of digital signature, 2013[2]** -In this research article the author's main aim of this study is to analyze the evidently value, legality and constitutional validity of digital signature in India.
- **Abhudaya A, Prithwajit G. use of digital signature in public interest, 2015[3]** -In this research article, the authors dissent the idea of the digital signature under the Information technology act. It helped me with getting a summary about the positive impacts of digital signature.
- **Payal Saha, digital signature analysis: An analysis of various Judgements of Indian Judiciary[4]** -In this research editorial, the authors has researched on both negative and positive feature of digital signature in legal systems, they have also study a variety of judgements to throw light on the outlook of this technique in India. It helped me to come across on a broader potential of the digital signature by studying both positive and negative implications and it also helped me to understand the matter and concerns of Indian judiciary by going through a variety of judgments.

CHAPTERIZATION

1. **Digital Signature understanding in brief: Technical Perspective-** This chapter deals with the procedure of digital signature. It also briefly talks about the authorities involved in the digital signatures.
2. **Positive aspect-** This chapter deals with the various positive aspects of digital signature

[1] Hanscom B, Digital Signature Impact , INFORMATION TECHNOLOGY LAW NETWORK, (September 15, 2010, 9:05 AM) https://www.academia.edu/37640493/A_Study_on_Importance_of_Digital_Signature.
[2] Dr. Dharmendra Kumar Singh, Constitutionality and Evidentiary value of digital signature, 55 INFORMATION TECHNOLOGY LAW JOURNAL 259, (2013).
[3] Abhudaya A, Prithwajit G., Use of digital signature in public interest, 26 SINGLE PROCESSING AND INFORMATION TECHNOLOGY LAW JOURNAL 125, (2015).
[4] Payal Saha, Digital Signature Analysis, 29 DIGITAL SYSTEM AND INFORMATION TECHNOLOGY LAW JOURNAL 135, (2013).

ISSN: 2582-6433

and its impact for creating safe environment for electronic transactions.

3. **Digital signature and its admissibility in court-** This chapter deals with a range of judicial pronouncements which will provide insights into the target of the judiciary and the application of the digital signature in the Indian judicial system.
4. **Judicial pronouncement in court-** This chapter deals with a variety of judicial pronouncements which will provide insights into the objective of the judiciary and the application of the use of the digital signature under the information technology act in the Indian judicial system.
5. **Conclusion-** It puts forward the conclusion of the attempts to answer the questions of the impact and the use of the digital signature under the information technology act and its legal effect.

LIST OF CASES REFERRED

1. Mr Madhukar G Angur vs M/S Alliance Business School on 28 March, 2018.[5]
2. M/S. Scania Commercial Vehicles vs Government of Karnataka on 10 November, 2016.[6]
3. Parminder Kaur vs State of U.P. and Another on 26 October, 2009.[7]
4. Paradigm Geophysical Pty Ltd. vs Commissioner of Income Tax.[8]
5. Hero Wind Energy Private Limited vs Inox Renewables Limited & Anr.[9]
6. Smt Shaila Chebbi Govind vs The State Of Karnataka.[10]
7. M/S. Hero Motocorp Ltd vs Union Of India & Ors.[11]
8. Ito vs M/S Allied Perfumers (P) Ltd.[12]
9. Cri. Rev. No.157/14 vs M/S Orion Infrastructure Ltd.[13]
10. L & T Hydrocarbon Engineering Ltd. vs Oil and Natural Gas Corporation.[14]

Electronic Signature – Legal and Technical aspect

The traditional signatures are hand written and are uniquely representative of one's identity. The use of signature is compulsory in law in certain cases and holds a considerable legal position in

[5] AIR 2018 SC 298.
[6] AIR 2016 SC 257.
[7] AIR 2009 SC 266.
[8] AIR 1984 SC 1473.
[9] AIR 1936 SC 295.
[10] AIR 2005 SC 1446.
[11] AIR 2010 SC 265.
[12] AIR 1933 SC 283.
[13] AIR 2013 SC 1339.
[14] AIR 1981 SC 1473.

ISSN: 2582-6433

the document as it indicate two things, the identity of the person and its intent to it. The Signature is one's identity on a document and is used in day to day transaction and in case of illiterate persons its fingerprint is considered as his signature. "The handwritten signature is prone to forgery and tampering hence insufficient for online transaction and contracts." The online transaction requires unique and strong protection which is served by electronic signature. "The concept of digital signature was introduced through Information Technology Act 2000 in India, which is enhanced with hybrid concept of electronic signature which is based on UNCITRAL Model Law on Electronic Signatures 2001." The electronic signature is a technologically neutral concept and includes a digital signature. The object and purpose of electronic signature are similar to that of traditional signature. "In cyber world electronic signature ensures that the electronic records are authentic and legitimate as electronic signature are safer and cannot be forged and is convenient as the sender himself does not have to be present personally at the place to contract to sign the document." For example a person can sign a contract in India and send it to any part of the world to complete the transaction.

UNCITRAL Model Law on Electronic Signatures 2000

The function of UNCITRAL Model Law on Electronic Signatures 2001 provides subsequent statement which signifies the value of electronic signature. The enhanced use of electronic verification techniques as substitutes for handwritten signatures and other traditional authentication procedures has recommended the need for an exact legal framework to reduce improbability as to the legal consequence that may result from the use of such modern techniques. Section 2(a) of Information Technology Act has defined electronic signature. The definition of electronic signature includes digital signature and new electronic technique which may be specific in the second schedule of the Act, thus an electronic signature means verification of electronic evidence by a subscriber by means of electronic techniques.[15]

The implementation of 'electronic signature' has made the Act technical impartial as it recognizes both the digital signature technique based on cryptography technique and electronic signature using new technologies.

Technical aspect of Digital Signature

The digital signature is formed and confirmed by using the Public Key Infrastructure (PKI)

[15] Mridul Kumar, An analysis of electronic signature in information technology, 16 STUDY AND ANALYSIS OF ELECTRONIC SIGNATURE JOURNAL 2453, (2010).

ISSN: 2582-6433

knowledge that requires two keys that is a public key and a private key for encrypting and decrypting in sequence. The significance is encrypted with a public key can only be decrypted by means of the equivalent private key and vice versa. The unique feature in public key infrastructure is that the public and private keys are related to each other and only the public key can be used for encrypting messages that can be decrypted using the corresponding private key. "The public key is shared, whereas the private key is known only to its possessor." The digital signature is based on Cryptography. Cryptography is the science to secure communications by converting the message (encrypting) into an unreadable format and only the person with a secret key can decrypt (read) it.[16] Cryptography systems can be broadly classified into two types i.e., symmetric-key and asymmetric.

"In symmetric systems, both the sender and recipient have same keys and asymmetric system each user has two keys a public key that is known to everyone and a private key that is known only the recipient of messages." In India signature uses an asymmetric system that has a public key and private key.

Digital Signature Certificates

Digital Signature Certificates are digital format certificate to establish individuality in the digital world. The digital signature certificates are issued by Certifying powers that be under the power of Controller of Certifying Authorities. A Digital Signature Certificate is an electronic document that can be used to verify that the public key belongs to the particular individual.

Digital Signature Certificates contains communal key of the certificate owner, Name of the owner, Validity "from" and "to" dates, Name of the issuing authority, Serial digit of the certificate, Digital mark of the issuing authority name of the person, etc. There are three diverse classes of digital certificate. Depending on the type, each digital certificate provides precise functions.

Legal aspect Digital Signature

Section 3 of the Information Technology Act 2000 provides for verification of electronic records. It provides that the electronic report can be authenticated by using digital signatures. It lays down expertise requirements for digital signatures. It makes use of an asymmetric crypto system and

[16] Vinayak Singh, Use of cryptography system in public interest, 25 DIGITAL SYSTEM AND INFORMATION TECHNOLOGY LAW JOURNAL 125, (2015).

ISSN: 2582-6433

hash function for authentication of electronic proceedings. Authentication of an electronic document is vital as it ensures that the proceedings has not been tampered and confirms the creator's individuality, making it non reputable, i.e., the sender cannot reject its creation.[17] The purpose of authentication is achieved by the use of asymmetric system and hash function which convent the electronic message into an incomprehensible format to avoid tampering of electronic record.

A hash function is the technique or scheme used for encrypting and decrypts digital signatures. A hash task produces a confusing value which is also known as a message digest. It plays a significant role in ensuring that the message has not been tampered and in sequence is safe and secure.

Functions of Electronic Signature

The idea of electronic signature was introduced under section 3A of the Information Technology (Amendment) Act 2008. An electronic signature means authentication of electronic evidence by a subscriber by any means of electronic verification techniques. An electronic signature technique can be used as an authorized electronic signature if such technique is notified by the central government in the official gazette or in the second schedule of the Act. There are different types of electronic signature, however, all of them are not secure; hence only the techniques notified in the official gazette or in the second schedule can be used as a legitimate electronic signature. The electronic signature technique has to be dependable to be recognized as an electronic signature. Section 3A of the Information Technology Act 2000 is based on Article 6, fulfillment with a requirement for a mark of UNCITRAL Model Law on Electronic Signatures 2001.

The following are the conditions of an electronic signature:

- It has to be dependable.
- The central government may inform in the official gazette the method and process for electronic signature or identify in the second schedule of the Information Technology Act 2000.

[17] Prashant Singh, Digital and Evidentiary value of digital signature, 45 INFORMATION TECHNOLOGY LAW JOURNAL 259, (2013).

ISSN: 2582-6433

An electronic Signature shall be measured as reliable if it fulfills following requirement:

- The technique should be such that it can be connected to the creator of the message.
- The technique of electronic signature must be under the power of the maker of the signature.
- Any change or modification to the electronic signature after affixation must be detectable.
- Any change or adjustment of data after affixing electronic signature must be visible.

The Central Government is the authority to state the technique as reliable electronic signature and can add or take away any technique from the electronic authentication technique.[18] The central government has not issued any announcement on the idea of electronic signature and thus the electronic name has not gained much attention. In this observation the Delhi high court has aimed at the central government to surround policy on electronic signature for authentication of electronic proceedings. "The only method of authentication of electronic records in India is presently being digital signature as there are no guidelines." The legal acknowledgment of electronic name has been provided under section 5 of information technology Act 2000. This section equates electronic signature as normal handwritten signature. It provides that if any, in order or document if confirmed by electronic signature.

Offences related to Electronic Signature

The offenses related to electronic signature are usually connected identity theft, journal of false electronic signature certificate, journal of electronic certificate with fake purpose. Section 66C of the Act punishes for individuality theft. This Act punishes fraudulent use of electronic signature of any other person and such person shall be punished with imprisonment of up to three years and will also liable to pay fines which may extend up to one lakh. "Misrepresentation or suppression of material fact in order to obtain any license or electronic signature is an offense under section 71 of the Act."

This section is relevant in the following cases:

- If a person makes a misrepresentation to the Controller or Certifying authority.
- If a person suppresses any material fact from, the Controller or Certifying authority.

[18] Dhruv Mukerjee , Digital Signature and electronic signature legal Impact , ELECTRONIC SIGNATURE AND TECHNOLOGY, (July 10, 2009, 8:10 AM) https://www.ijcsmc.com.

ISSN: 2582-6433

Such falsification or suppression of matter fact with the intent to obtain any license or electronic certificate from, the manager or Certifying authority is carrying a punishment of imprisonment of up to two years and fine up to rupees one lakh.[19] The series to be provided to the Controller or Certifying authority should be good and right. Journal of electronic signature certificate which is forged in certain facts is an offense under section 73 of the Act.

The following shall amount to journal of false details:

- Publication of Electronic signature certificate which the certifying power has not issued.
- Publication of Electronic signature certificate which subscriber of the certificate has not established.

"Sec 74 of the Act punishes creation, publication or providing of electronic signature certificate for fraudulent or unlawful purpose with imprisonment for a term which may extend up to two years or a fine which may extend up to one lakh." The budding online transactions and contracts require stronger defense which is currently fulfilled by digital signature. However, it would be in the attention of cyber community if the Government allows and start multiple method of verification like the use of fingerprint or aadhaar card connected with password based online deal. "The multiple methods would permit easy identification of persons which will assist in curbing online frauds and ease online transaction and further enhance online security of users as to even today the factual identity of persons online is a mirage." India passed Information technology Act 2000 (The Act) which came into force on 17-10-2000. The Act applies to the whole of India and even to persons who commit offence outside India. The Act validates digital signature and provides for enabling a person to use it just like the traditional signature.[20] The basic reason of digital signature is not dissimilar from our conventional signature. The reason therefore is to validate the document, to be familiar with the person and to make the inside of the document obligatory on person putting digital signature. A digital name or digital signature scheme is a mathematical scheme for representing the authenticity of a digital message or file. A suitable digital signature gives a receiver reason to consider that the message was created by a known sender, and that it was not indistinct in transit. Digital signatures are based on collective key encryption. The performance of DS is based on the scheme of community key cryptography.

[19] Prashant Singh, Digital and Evidentiary value of digital signature, 45 INFORMATION TECHNOLOGY LAW JOURNAL 259, (2013).
[20] Prasanna Kumar, An analysis of digital signature in information technology, 13 STUDY AND ANALYSIS OF DIGITAL SIGNATURE JOURNAL 2245, (2001).

ISSN: 2582-6433

Public-key cryptography refers to cryptographic scheme requiring two divide keys, one of which is secretive and one of which is public. Although different, the two parts of the key pair are mathematically linked. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

Key encryption allows more than just privacy. It can also assure the recipient of the authenticity of a document because a private key can be used to encode a message that only a public key can decode. Justice Yatindra Singh in his book 'Cyber laws' has established that since shared key encryption is time-consuming and the hash function is used to change a note into a unique shorter lasting length significance called the Hash result. "Hash serves the purpose of an index of the original text. It is an algorithm mapping or translation of one sequence into another." The hash function is such that the same hash result is obtained every time that hash function is used on the same electronic record and two electronic records cannot produce the same hash result using the same hash function. "In other words mapping is one to one and not many to one." It is one way and cannot rebuild the original communication from the hash result. The encryption of a hash result of the message with the private key of the sender is called a digital signature.

DIGITAL REVOLUTION IN INDIA

In India, MCA-21 plan launched by the Ministry of Corporate Affairs (MCA) really transform the use of digital signature by making E-filing obligatory for most of the credentials required to be filed under the Companies Act 1956 and under the Limited Liability Partnership Act 2008 (LLP Act). The Income tax department followed suit and provided compulsory filing of returns in the electronic mode except a few under the Income Tax Act 1961.[21] The Central Excise Act and Finance Act 1994 (operate with service tax) also provide for schemes for E-filing. "Now the application for registration under Foreign Contribution Regulations Act provides that it shall be filed electronically." The application for IEC code is to be filed electronically with DGFT (Director General of Foreign Trade). In Kerala the Department of Commercial Taxes mandates E-filing of returns using DS under the Kerala Value Added Tax Act 2003. In India, other states also amended their VAT laws to make provision for E-filing. Likewise under the Partnership Act 1932 also, firm registration application is to be filed electronically.

[21] Sawant Jain , Brief of electronic signature in information technology, 10 STUDY AND ANALYSIS OF ELECTRONIC SIGNATURE JOURNAL 2353, (2009).

ISSN: 2582-6433

The discussion above indicates the extent of electronic revolution that has taken place in India and thus the significance and relevance of digital signature.

ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE

On a closer examination it can be noticed that the expression electronic signature is very wide and digital mark is only one of the many kinds of electronic signatures one can envision. The term electronic signature is defined under section 2(a) of the IT Act 2000 (as inserted by Information Technology Amendment Act 2008 (ITAA) as follows –

1) Electronic signature means verification of any electronic evidence by a subscriber by means of the electronic method specified in the second agenda and includes digital signature.

The expression Digital signature is defined under section 2(p) as follows –

2) Digital Signature means verification of any electronic evidence by a subscriber by means of an electronic method or process in accordance with the supplies of section.

Therefore electronic signature is a wider word and digital signature is one type of an electronic signature under the IT Act 2000. "The person can always say that some other person typed his name in the document without his consent or knowledge." Here, the digital signature plays an important role as the same is secure and the person cannot be allowed to deny that he did not sign unless he prove with clear evidence that it was put without his consent or knowledge.

DIGITAL SIGNATURE CERTIFICATE (DSC)

Digital Certificates provide as an identity of an individual for a certain purpose, e.g. a driving license identifies someone who can legally drive in a meticulous country. Likewise, a Digital Certificate can be presented electronically to prove your identity or your right to access information or services on the Internet.[22] Digital Certificates are the digital equivalent (i.e. electronic format) of physical or thesis Certificates like driving license, passport or membership cards.

Section 2(q) of the Act explains about the term Digital Signature Certificate. A Digital Signature

[22] Prasanna Kumar, An analysis of digital signature in information technology, 13 STUDY AND ANALYSIS OF DIGITAL SIGNATURE JOURNAL 2245, (2001).

ISSN: 2582-6433

Certificate issued under sub-section (4) of section 35 and does not give details its meaning. DSC is issued by the organization known as CA (Certifying Authorities). "Section 35 deals with the procedure for issue of electronic/digital signature by the Certifying Authorities (CA)." Section 35(4) provides that on getting of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other declaration under sub-section (3). After making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing declines the application provided that no application shall be discarded unless the applicant has been given a reasonable opportunity of showing cause against the proposed denial. "Thus the IT Act 2000 as such does not contain the exact value of the term Digital Signature Certificate but only describes that such a certificate is one which is issued by the CA after following the prescribed procedure."

TYPES OF DIGITAL SIGNATURES

There are three types of digital signatures based on safety levels like Class-1, Class-2 and Class-3 certificates. Class 1 certificates do not carry any legal recognition since its validation is based only on the basis of a valid e-mail and is not based on direct verification. In the case of Class-2 certificates the identity of the person is verified on the basis of a trusted pre-verified database.[23] Class-3 represents the top level where a person is necessary to be present in front of a RA (Registration Authority) to establish his/her identity.

MCA 21 insists on Class-2 certificate for filing credentials under the Companies Act and Limited Liability Partnership Act. The other authorities also recognize Digital Signature Certificate in the class-2 category and not class-1. "The Digital Signature is necessary under the Companies Act and LLP Act by auditors, directors, company secretaries, bankers (for filing registration and approval of charges) for the purpose of filing various returns and documents." The Digital Signature Certificate once issued is normally valid for 1 or 2 years and can be renewed on its expiry.

DIGITAL SIGNATURES AND EVIDENCE ACT

The Indian Evidence Act 1872 is a part of legislation dealing with evidences that can be shaped or admitted in a court of law by the litigating parties. "The law which was enacted in 1872

[23] Piyush Rai, An analysis of digital certificate in information technology, 20 STUDY AND ANALYSIS OF ELECTRONIC SIGNATURE JOURNAL 2453, (2013).

ISSN: 2582-6433

naturally did not envisage electronic signatures and records as evidences." Hence in view of the widespread use of electronic records and Electronic signatures including Digital Signature it was felt essential to amend the said Act to make it in conformity with the changing trends in the society. Section 3 of the Evidence Act 1872 provides for interpretation or definition of certain words or expressions used in the Act. "The said section was amended to include electronic records also in the definition of the term evidence." Further section 47A has been inserted to provide that when the Court has to form a view as to the electronic signature of any person, the opinion of the Certifying Authority which has issued the electronic Signature Certificate is a relevant fact.[24] Section 67A has been inserted which protects the safe electronic Signature.[25] It provides that if the electronic mark of any subscriber is believed to have been affixed to an electronic verification the fact that such electronic signature is the electronic signature of the subscriber must be proved except when the similar is a secure electronic signature. Section 73A has been newly inserted to offer that the court may direct the concerned person or Certifying Authorities (CA) to determine whether Digital Signature is that of the person by whom it is purported to have been affixed. "It may also direct any other person to apply the public key listed in the electronic Signature Certificate and verify the electronic signature purported to have been affixed by that person." Section 85B(1) provides that In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates. "Section 85B (2) provides that unless the contrary is proved the court shall presume that the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record." It further provides that there shall be no presumption relating to authenticity and integrity of the electronic record or any electronic signature if the same is not secure.

Section 85C deals with situations where the Court shall believe, unless contrary is proved, that the information scheduled in an Electronic Signature Certificate is right, except for information specified as subscriber information which has not been verified, if the certificate was established by the subscriber.

[24] Rakesh Bhagat, Brief of Section 67A and the evidentiary value of digital signature, 45 INFORMATION TECHNOLOGY LAW JOURNAL 295, (2015).
[25] Yogesh Goel, Information on the certifying authority system, 29 DIGITAL SYSTEM AND INFORMATION TECHNOLOGY LAW JOURNAL 135, (2013).

ISSN: 2582-6433

DIGITAL SIGNATURES AND THE INDIAN PENAL CODE

Indian penal code 1860 (IPC) is in procedure in India very effectively for the last 152 years. Nobody seriously felt the need for an amendment because of its outstanding draughts man ship. But a need was felt for adding up of certain supplies to take care of the new developments in the field of electronics and information proficiency. Thus through the Information Technology Amendment Act 2008 IPC was also amended. The salient features of the amendments are discussed below: Section 73A has been inserted to present the same provision as in section 47A of the Indian evidence Act. "Section 464 has also been amended to provide that the said section shall be made applicable to electronic records and electronic signatures also." Section 464 deals with situations when a person is said to make fake papers or electronic records. Section 466 provides for forging of electronic records also. There are amendments to sections 4, 40, 118, 119 also which are not dealt with in this article for want of space.

CONCLUSION

The advent of signatures has given individuals a distinct identity and enabled the business sector and other persons to perform more quickly, keeping up with evolving technology. Signatures have by far played a significant part in individual decision making and consent at a considerably higher value. Historically, each individual or authorized signing was required to read the document in its entirety before providing his agreement. This presented enough challenges for the organizations to keep up with the signatory's speed and circle around his/her timeframe. The Authorised Signatory may not be present at a certain location but yet provide his agreement. Technology has generously given for him. By the technological advancements, the use of digital signatures instead of traditional signatures has grown significantly. The Information Technology Act of 2000 discusses the notion of digital signatures, the authorities who have been given the authority to issue digital signature certificates, and the situations that necessitate the affixation of a digital signature.

REFERENCES

- Computers, Phones, and the Internet: Information Technology, by Jennifer in Security Journal, 1940
- G. Feghhi, P. Williams, Electronic Certificates: Applied Internet Security, MA, 1949.
- Information Technology, Corporate Productivity, and the New Economy, by Vikram Diwan, 2010.

ISSN: 2582-6433

- Information Technology Development: A New Paradigm for Delivering the Internet to Rural Areas in Developing Countries with the use of digital signature, by Jeffrey James.
- Information Technology's Management and Business Processes and Inter-Organizational Relationships and Extend the Concept of Community-Particularly for Our People-Oriented Institutions, by Ronald, 2015.
- L. Bishop, Introduction to Computer Security, MA, Wesley, 2003.
- Rao V, Network Security: Private Communication in a Public World, 2003.
- Singh P, Security in Computing, 2002.
- The Digital Impact and Condition: Culture in the Information Network, by Mridul Pathak, 2003.
- V. Stallings, Cryptography and Network Security, NG, Englewood, 2001.