



Wet Signatures to Digital Signatures

TBA BULLETIN SPECIAL EDITION

Signatures, the act of signing one's name to something. The evolutionary process of signatures have been deep and interesting but the inherent value and it's significance of it has remained unchanged.

Signatures go back to 3000BC ancient scribes adopted by the Sumerians and Egyptians. This were to denote identity of tribe members. Not much has changed to modern day electronic signatures, used to complete and validate important financial transactions, contracts through the online domain and now smart contracts and even blockchain.



A Sumerian clay tablet of 3100BC consisting of series of pictures, symbol, pictographs are today considered the earliest definitive examples of using symbols to denote identity. The importance and significance of signatures have evolved from one era, depending largely on the subject of utility during that era. The development of language by Romans and Greeks was pivotal during 1200BC. The Greeks developed the Phoenician alphabet to communicate which evolved into the Latin alphabet which we know today. Latin contributed to the development of what is the prevalent signature in the period of El Cid, a Medieval military leader who used his own signature to validate the donation he made to the Cathedral of Valencia. Thus, the first documented signature in the history of mankind, was born.



Modern Signature

In 1677, the English Parliament passed The Statute of Frauds Act, which marked the birth of signatures as the law created a mandate that in case of validation of contracts, signature of the parties involved are mandatory. Enforcing this law meant curbing fraudulent documentation and contracts prevalent in England, then.

The signature of John Hancock on the American Declaration of Independence in 1776 turned out to be the most recognizable signature in the history of mankind during that period. A landmark event, for two reasons, denotation of the signature in the American Declaration of Independence and for the first time signature symbolizing and representing a binding contract between parties.

Technology, has changed a lot and introduced a lot of redundancy but signatures have metamorphosised and had upgrades- and yet remained.

During 1980s-2000s contracts started getting scanned electronically to the other party through fax machines, this was the first version of digital signatures. Legislations had to come to the aid of modern day signatures.

Electronic Signatures And Digital Signatures



In short, a digital signature is a type of electronic signature.

An electronic signature is an electronic symbol attached to a contract or any record, by a person with an intent to sign. In contrast, digital signatures rely on algorithms and cryptography to provide integrity to a signature, it guarantees that an electronic document is authentic.

Legislatures which govern e-Signatures in some countries:

Canada: The Personal Information Protection and Electronics Documents Act;

China: E-Signature Law;

EU: The Electronic Identification and Authentication and Trust

India: The Information Technology Act, 2000



It appears a recent phenomenon, but the idea of electronic signatures came into existence way back in 1976 by Whitfield Diffie and Martin Hellman. The theory suggests the creation of two algorithmic keys which includes one to be public key which will be open for the general public at large and the other will be a private key which will remain with the original user and will be used in order to decrypt the source. The theory highlighted the importance of security in a transaction especially done over the online domain and in order to maintain security it was suggested that only one key will be produced which shall remain with the original user and not to general public at large. Slow moving technology during 1976 to 1990s contributed to the creeping development of electronic signatures. Digital signatures loomed as ideas.

The broad difference between Digital Signature and E signatures:

E Signature	Digital Signature
It is used through modes of e-mail, signature scans, phone verification, IDs of the signer	Certificate based and linked to signer identity for authenticity
Easy to implement	Complex for implementation
Equivalent to wet signatures	Not same as wet signatures
Can verify document authenticity	Secures document integrity
Audit is required to determine validity and legality	Authenticity is determined through encryption at each stage

India

There isn't any law prescribing method for stamping electronic documents in India, Maharashtra, Karnataka and Delhi have made it mandatory for an electronic document to be stamped.

All limitations have not been transcended, yet by electronic signatures. It cannot be used on:

- (i) a negotiable instrument especially a promissory note or a bill of exchange
- (ii) Trust Deeds
- (iii) Wills
- (iv) Lease Deeds or Sale Deeds.

The limitation indicate that electronic signature is inadmissible in the Court of law when used on the aforesaid legal documents. Only wet signatures can be used in order to validate and ratify the legal document and in turn will be considered admissible in the Court of law.

Digital Signatures

“Security” is the differentiator amongst the new adapted versions of signatures. Digital signatures warrant lesser security in comparison to wet or electronic signatures. A certificate of authenticity is required with the digital signature to increase its authenticity when attached to a document.

Once the digital signature is used, any form of change to the document becomes visible to the parties rendering the document/contract invalid.



It's basic functioning involves a public key cryptography also known as asymmetric cryptography. Asymmetric cryptography is based on the theory provided by Whitfield Diffie and Martin Hellman and it is an algorithm which allows a user to create two keys at once, a public key and a private key linked together through the algorithm. The user, can encrypt the data through the public key and to decrypt the user's public key is required. It creates a more secure and layered way for sharing of the information.

The usage of digital signature is preferred in smart contracts and blockchain as the degree of authentic and validation is higher. Blockchain is digital chain of blocks used for various purposes including storage of information about the user and of online transaction. Usage of digital signature in blockchain implies that the user makes the key public to the general public at large and in this case mostly Ethereum is used as an address book. Ethereum, an open sourced software platform which is based on blockchain, used to run smart contracts and other financial transactions over digital domain providing higher amount of security and control. The private key remains with the original user of the domain and only such original user can decrypt the transaction done over Ethereum and gain access to the funds generated out of the transaction. This makes the entire transaction done over the blockchain, secure with the decryption key only with the original user. The same mechanism works while authenticating a smart contract with a digital signature.

Conclusion

With the immense development in technology, most of the world known to mankind is set to change, but signatures are set to evolve while retaining what they convey.

Transitioning from one form to the other, they remain as important and convey the same meaning. All hope is not lost for the wet signature, since they remain the way to ratify and authenticate key legal documents including Lease deeds, Sale Agreements, promissory notes, Judicial Orders and Powers of Attorney

Disclaimer:

This Note is for general information only and not intended for solicitation.

Please do not treat this as a legal advice of any sort. Views contained in this, are personal with interpretive value of the author and teams assisting the author.

Readers are encouraged not to rely solely on these contents before making any decision.