Whitepaper

Adding 'e to life: Conveniences and Complexities

By Mustafa Syed

Signature – The definition

If somebody had asked me as to when was the first time I signed my name I am not able pin point the exact date but I am sure that at a very early age I did practice to have a unique way of writing my name (signature) to be able to affix it to documents such as letters, cheques etc to associate an identity or to provide proof of my consent.

I also have recollection of cutting out certain marks in a potato to create a seal that could be used to print exactly identical mark every time I wanted to sign and seal a document.

Till today I have a vivid remembrance of my need to sign my name in such a way that my friends couldn't imitate it and I could proudly challenge them that it could not be forged.

It was only until late that I learnt; how signature were used, what it legally meant by signing a document etc. today when I am looking for a single sentence to define and describe a signature I end up finding a list of definitions descriptions. Though you may find some of them similar in meaning and significance some are by far not close to the common understanding of the word Signature.

A Signature is;

1. One's name as written by oneself.

2. The act of signing one's name.

3. A distinctive mark, characteristic, or sound indicating identity.

4. A signature is a usually stylized version of someone's name written on documents as a proof of identity, like a seal, but handwritten.

5. Text automatically appended to E-mail and Newsgroup messages, usually including a name, contact info, and sometimes quotes and ASCII Art, is also called a signature. See Signature block.

6. To write one's name to an instrument of writing in order to give the effect intended; the name thus written is called a signature.

7. By signature is understood the act of putting down a man's name, at the end of an instrument, to attest its validity. The name thus written is also called a signature. It is not necessary that a party should write his name himself, to constitute a signature; his mark is now held sufficient though he was able to write. A signature made by a party, another person guiding his hand with his consent, is sufficient.

8. Japanese culture does not have signatures, per say, but uses name seals with the name written in tensho or seal script.

Today it amazes me to learn that forensic experts can to a great extent identify who actually singed a particular document or at least who did not write the signature in question by identifying unique features provided to us by nature. Alas, all my effort to create a unique signature is wasted.

Signature – Attributes

1. The traditional function of a signature is evidential: it is to give evidence of
    a. the provenance of the document; and
    b. the intention of an individual with regard to that document. For example, the role of a signature in many consumer contracts is not to provide evidence of the identity of the contracting party, but rather to provide evidence of deliberation and informed consent.

2. Signatures may be affixed by a party to provide evidence of agreement and deliberation of another party. For example signing "for and on behalf of"

3. Signatures may be witnessed and affixed in the presence of a Notary Public.

4. Specimen signatures may be maintained in depositories and registries. For example signature registries maintained by Notaries in certain parts of the world.

5. Specimen signatures may be published for validation and verification. A good example would be specimen signature book of the staff published by banks.

Looking at the list above it clearly identifies the minutiae of the mechanism used today for affixing and verifying signatures, determining the responsibility and liability, associating a natural person to a legal entity as "authorised" to act "for and on behalf of".

For centuries the above practices have been part of our approach for formulating a framework, have matured with time and are widely supported by customs, practices and legislations throughout the globe while they may maintain certain unique attributes to cater for the local peculiarities.

Signature – The Legal Force

The provision of warranties, indemnities, protections and mechanism for dispute resolution various legislations throughout the globe have not only recognized the signatures as a tool for ascertaining an identity, intent and responsibility of a party in a dispute they have even defined the signatures in a variety of manners to cover for the peculiarities of various documents, contracts, agreements and instruments. The signature not only adds moral commitment to a document it also adds legal responsibility of the party.

Though the legislations of all civilized countries provide for non-repudiation of association, intent and commitment by the signing party these also maintain check and balance and provide for a mechanism to repudiate if it can be proven beyond doubt that certain conditions existed at the time of signing. For example a person cannot be held responsible for signing while a gun was held against his head.

The Information Age – Signature not necessary

Most of us have seen in a few decades how the automation has pushed the information age to its current state. This era of gathering more and more information, converting it to knowledge and delivering it to end-user as fat as possible also affected our age old habit of depending solely and firmly on signatures for guaranteeing association and commitment of the parties involved.

I believe most of us have come across documents displaying a message "*This is a computer generated document and does not require signature*" while maintaining space for "Authorized Signature" (a dotted line).

Due to missing equivalent electronic signature to sign documents in electronic format various methods were worked out. For example; telex systems provided authentication of the sender through answer-back messages, symmetric keys, pre-agreed number tables and algorithms provided mechanism to verify integrity of messages while all this was still supported by internal paper documents that were signed and counter-signed.

The communication networks were still private, used only by authorized users and systems deploying hybrid solution based on paper documents with hand-written signatures and electronic messaging systems were utilized to add efficiencies to existing ways of doing business.

e-commerce – The definition

Though the concepts of e-Commerce, electronic documents and transactions over shared public networks may be a development of last decade or so but early electronic transactions may have happened as early as 1880s when Richard Warren

Sears use to receive his orders through telegraph for mail order business he had established.

Though this section is out of scope of the matter being discussed here, it is only included to provide some feel of how important e-signature can be to move forward in direction that businesses have taken in last few decades. Following definition will provide you enough insight to delve deep into the way business is being done today.

E-Commerce (EC): The conducting of business communication and transactions over networks and through computers. As most restrictively defined, electronic commerce is the buying and selling of goods and services, and the transfer of funds, through digital communications. However EC also includes all inter-company and intra-company functions (such as marketing, finance, manufacturing, selling, and negotiation) that enable commerce and use electronic mail, EDI, file transfer, fax, video conferencing, workflow, or interaction with a remote computer.

e-signature – The definition

A digital signature is an electronic (code) signature that can be used to authenticate the identity of the sender of a message or the signer of a document and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

A more formal definition: "(I) A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

(II) Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient."

Source: IETF (http://www.ietf.org/rfc/rfc2828.txt).

e-signature – How it works (with PKI)

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.

2. Using special software, you obtain a message hash (mathematical summary) of the contract.

3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.

4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.

2. Your lawyer then uses your public key to decrypt the message hash or summary.

3. If the hashes match, the received message is valid.

e-signature – Legislation & Legal Status

1) US Federal: In June 2000, President Clinton signed the Federal Electronic Signatures in Global

and Network Commerce Act ("E-Sign"). The E-Sign act extends nationally what had been implemented by many states through UETA. E-Sign does not aggressively promote or extend the use of electronic signatures. Rather, E-Sign is protective, in that it "assures electronic signatures, contracts and other records shall not be denied legal power and enforceability on the sole ground they are in electronic form." Electronic signatures carry the same legal weight as those on paper, but the Act does not mandate the use of electronic signatures.

a) E-Sign is very broad about what specific technology can be used to create the signature, and does not contain technical requirements. Public-key encryption is not mandated as a requirement, and other technologies, such as biometrics, could be used.

b) Some document types are exempted from E-Sign. Electronic documents concerning wills, adoption, and divorce, for example, are exempted.

2) US State: Uniform Electronic Transactions Act (UETA) is legislation that has been enacted by several states. Though states can introduce variations into the statute, UETA is an attempt by them to enact common interstate legislation. As of July 2001, 37 states had enacted UETA. UETA was the model for E-Sign so there are many similarities. As with E-Sign, UETA grants electronic signatures legal enforcement but does not mandate their use. No technical requirements are made and documents concerning wills, adoption, divorce, and other topics are exempted from this legislation.

3) International: In 1999, the European Union adopted a Directive on a Common Framework for Electronic Signatures. Unlike the US approach, the EU framework is more specific. It provides wording that details how digital signatures need to be stored for authenticity and non-repudiation. It strongly advocates that digital signatures be stored in tamper resistant devices (i.e., smart cards.) Each EU country will develop its own laws within this framework.

Local: in 2002 Government of Pakistan promulgated a law; Electronic Transaction Ordinance (ETO) 2002 to recognize digital documents, certificates and signatures as equivalent to paper documents and written signature. The legislation recognizes all files/ data in any electronic format as documents and that these documents shall not be denied legal power and enforceability.

ETO-2002 – Brief encounter (Pakistani legislation)

1) Legal recognition of electronic signatures.

a) The requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signatures are applied.

2) Proof of electronic signature.

a) An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both.

3) Presumption relating to advanced electronic signature.

a) In any proceedings, involving an advanced electronic signature, it shall be presumed unless evidence to contrary is produced, that:

i) the electronic document affixed with an advanced electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; or

ii) the advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time.

4) Stamp Duty.

a) Notwithstanding anything contained in the Stamp Act, 1899 (II of 1899), for a period of two years from the date of commencement of this Ordinance or till the time the Provincial Governments devise and implement appropriate measures for payment and recovery of stamp duty through electronic means, whichever is later, stamp duty shall not be payable in respect of any instrument executed in electronic form.

5) Attestation and notarization.

a) Notwithstanding anything contained in any law for the time being in force, no electronic document shall require attestation and notarization for a period of two years from the date of commencement of this Ordinance or till the time the appropriate authority devise and implement measures for attestation and notarization of electronic documents, whichever is later.

6) Certified copies.

a) Where any law requires or permits the production of certified copies of any records, such requirement or permission shall extend to printouts or other forms of display of electronic documents where, in addition to fulfilment of the requirements as may be specified in such law relating to certification, it is verified in the manner laid down by the appropriate authority.

7) Application to certain laws barred.

a) (1) Subject to sub-section

(2) nothing in this Ordinance shall apply to:

i) (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (XXVI of 1881);

ii) a power-of-attorney under the Powers of Attorney Act, 1881 (VII of 1882);

iii) a trust as defined in the Trust Act 1882 (II of 1882), but excluding constructive, implied and resulting trusts;

iv) a will or any form of testamentary disposition under any law for the time being in force; and

v) a contract for sale or conveyance of immovable property or any interest in such property.

b) (2) The Federal Government after consultation with the provinces may, by notification in the official Gazette and subject to such conditions and limitations as may be specified therein, declare that the whole or part of this Ordinance shall apply to the whole or part of one or more instruments specified in clauses (a) to (e) of sub-Section (1).

8) Repository.

a) (1) The Certification Council shall establish and manage a repository for all accreditation certificates, certificates issued by accredited certification service providers and for such other information as may be specified in regulations made by the Certification Council.

e-signature – The facts we all must know

It is evident from various definitions of e-signature and legislation enacted so far that almost everyone has tried to maintain technology independence so far. But generally it is also seen that use of PKI is catching up as a popular method of creating e-signatures (digital signatures) worldwide.

Use of PKI has some merits, over other methods, which are clearly seen as convenient and secure by the industry and businesses deploying such solution. The convenience of sharing keys, irreversible hashing algorithms and association of keys to an individual using digital certificate issued

by a trusted party (Certificate Authority) have mainly contributed to this wining recipe.

A Certificate Authority (CA) issues a digital certificate with the information provided by the certificate subject, verifies information provided for correctness, digitally signs this certificate, associates such certificate with a public key and also publishes this key through its repository.

Through intelligently drafted legal agreements CA also puts all the responsibility liability on the certificate subscribers and relying parties whereas most popular internet browsers and email clients provide mechanism to trust a certificate implicitly or explicitly.

In such scenarios it very important for all to make sure that the certificates are only trusted and relied upon if these are issued by a trusted CA and are validated by issuing authority as not expired and/or revoked. Adding any certificate explicitly to the trust list maintained by your operating system is no less than committing hara-kiri.

CA is required to publish its Certificate Policy (CP) and Certificate Practice Statement (CPS) along with other agreements such as Subscriber's Agreement & Relying Party's Agreement. Equally important is the fact that all parties must understand and exactly know indemnities and warranties listed in various legal contracts.

The digital certificate verifies that the key pair used for the digital signature is associated to the person whose information is provided in the certificate. The certificate may also associate a person to an enterprise as authorized signatory. This demonstrates total dependence on the trust relying party must have in the certificate issuing authority (issuing CA) and his ability to get the certificate verified from the CA. It is an accepted fact and recommended best practice to not trust a certificate that cannot be verified for its validity, this means the CA must provide online certificate validation in real-time. Any CA just providing Certificate Revocation Lists is not good enough for serious business.

Trusting a CA must always be a well-thought decision and must be based on good knowledge of the security of the CA itself, its policies and practices pertaining to certificate lifecycle management, hiring of staff, access to sensitive information and areas (physical access), segregation of staff duties etc.

An individual needing to rely on a digital signature should not have to be well-informed of all the legal and contractual intricacies on the contrary the individual will be more comfortable if there is some external entity that can audit and accredit certificate issuing CA as trustworthy. Luckily ETO-2002 provides for such mechanism, it recognizes the accreditation by the Electronic Certification Accreditation Council (ECAC) formed under the ETO-2002 as well as accreditation by other globally trusted ROOT certification authorities.

It is also worth mentioning here the parts where ETO-2002 fell short of completing the job and some matters that are impracticable and must be taken care of through notifications to set things right.

1. Sub-section 9(b) states "the advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time". Since ETO-2002 does not provide any mechanism for electronic attestation/ notarization or witness it is impractical to assume that the signature was affixed with any such intention.

2. Sub-section 23(1) states "the Certification Council shall establish and manage a repository for all accreditation certificates, certificates issued by accredited certification service providers and for such other information as may be specified in regulations made by the Certification Council". Currently Certification Council (ECAC) does not have its globally trusted ROOT certificate and economies of scale do not exist to allow ECAC to manage such mechanism it should be formally notified and postponed till such date when it will be viable for ECAC to fulfil such responsibility.

Now I would like to mention few things that ECAC can do, through official notifications as provided by ETO-2002, to facilitate the rapid acceptance of digital certificates and digital signatures for secure e-commerce and e-banking in the country.

1. On the same lines as provided by Electronic Signatures and Records Act (ESRA) Guidelines (USA), ECAC should provide Best Practices Guidelines to guide Certification Service Providers and maintain a certain minimum level of standard in the country.

2. These guidelines must define various classes of digital certificates with various levels of reliance for financial transactions and contractual documents.

3. These guidelines must also define minimum security and legal requirements for maintaining key escrows and similarly must emphasize on use of separate key pairs for signing and encryption. The necessity of maintaining such escrows is emphasized in later section.

4. The guidelines must emphasize on the usage of time & date stamping for all time critical transactions (e.g. transactions in online trading).

5. Last but not the least ECAC must devise a mechanism for notarization of documents if the intention of the signer is to be proven.

In fact all legal systems of the civilized world provide for "Repudiation" in certain conditions. The techies of the world have used and abused the word "Non-repudiation" so much that I strongly feel the need to explain normal practices by CA(s) that can give rise to serious doubts and may open this matter to number of possible interpretations.

Enterprises that use PKI for conducting secure business and issue certificates to their staff, customers or business partners would like to maintain a repository of all emails that their employees have received, some of which possibly are encrypted as well for confidentiality. Since the enterprise might want to decrypt these messages at some point in future, when either the employee has left or his certificates is lost with the associated keys, they prefer to maintain a key escrow where all private keys are securely stored and could be extracted when needed.

In a scenario where same key pair is used for digital signature as well as ciphering the message and these keys are stored in the secured escrow maintained by the enterprise, providing the proof beyond doubt that the access to keys was at all times restricted to the certificate subject only could be an uphill task thus raising serious doubts about the non-repudiation promised by this technology.

Conclusion

There is no doubt that we have come a long way in improving these technologies to provide the comfort and trust to parties conducting business through electronic documents and transactions from one end of the world to the other there is even more need for governance in a totally new territory for all of us. And I must also be content with these (web) technologies for providing such convenient ways of researching, collecting information and doing business with such speed that would not have been possible only a few decades back.

Secure Bytes Inc.
2961 Andrus Drive,
West Chicago, IL 60185
United States of America

www.secure-bytes.com