Process, Application and Authenticity of Digital Signature

Ms Himanshi A Chaudhary
MBA , IIIrd Sem
GFSU, Gandhinagar

Abstract

The use of digital signature or e-signature technology is increasing day by day in banking, insurance, corporate sector as well as in all fields of e-commerce, where use of electronic instruments / tools is necessary. Digital signature technology is cryptographic mechanism, used public key and private key, is very secure and sophisticated technology, which can be encrypted and or decrypted. This technology is for reducing the cost, to save time and speedup of work. Therefore, present paper is a review of work of different authors involved in the process of digital signature either for its mechanism or to take to the people of the country for its adoption or awareness about its use and advantages.

Key word: *digital signature, cryptographic mechanism, encrypted, decrypted*

Introduction

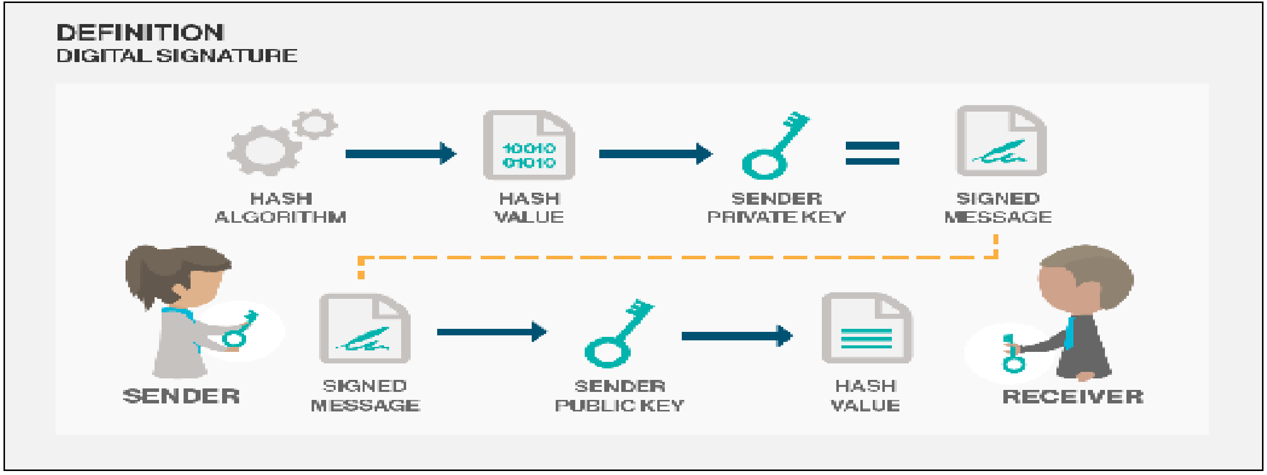
Digital signature is a paperless process through which individual can sign a document as he has to sign on paper with the help of electronic software, where two keys are generated viz ; (i) public key and (ii) private key. From these keys, one is confidential and is remains with the signatory i.e. private key, while other remains with the software used for the purpose known as public key. Both the keys are necessary to use this technology known as cryptographic system. A unique element to the public key system is that both the keys (public and private) are related in such a way that only the public key can be used to encrypt messages and only corresponding private key can be used to decrypt them. However, it is virtually impossible to deduce the private key, if you know the public key. This technology was invented by Whitfield Diffie and Martin Hellman in 1976 and also called as asymmetric encryption, because it uses two keys instead of one key (Anonymous, 2016).

Process of digital signature

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked i.e. (i) private key and (ii) public key. To create a digital signature, signing software creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash - along with other information, such as the hashing algorithm - is the digital signature. The reason for encrypting the hash instead of entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

A digital signature can be used with any kind of message - whether it is encrypted or not - simply so the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person or entity.

Figure -1: Process of Digital Signature



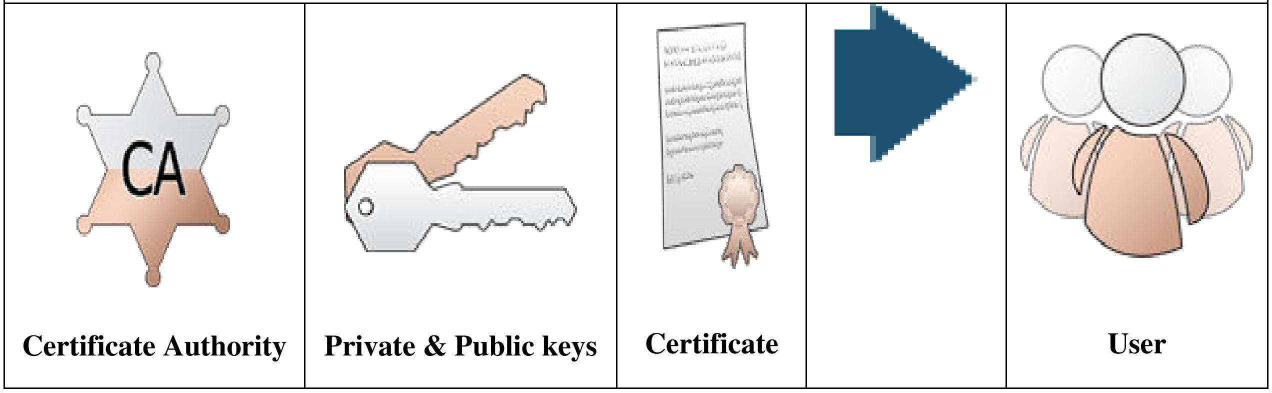
Source: Margaret and Michael (2014)

If the two hash values match, the message has not been tampered with, and the receiver knows the message is from sender. It is easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and non-repudiation of communications and transactions conducted over the Internet (Figure-1).

Generating private key

For digitally sign documents, user needs to obtain a Private and Public Key – a one-time process, it's done by Secured Signing Service, while user registered. The Private Key isn't shared and is used only by user sign documents. The Public Key is available for all, used for validate the signatory's digital signature.

Figure-2: Public and Private Key.



Source: Anonymous (2017)

Generating public key

Public Key Infrastructure (PKI) is a collection of technologies, processes, and organizational policies that support the use of public key cryptography to verify the authenticity of public keys. PKI provides the mechanisms to ensure that the trusted relationships are established and maintained.

Complex business systems, e-commerce and automated business transactions require robust and precise security procedures. While today's Internet client demands security to protect their interests, privacy, communication, value exchange, and information assets.

PKI enables users using insecure public network like Internet to securely and privately exchange data and do financial transaction through the use of public and private cryptographic key pair.

Important characteristics of key pairs

- While they are mathematically related to each other, it is impossible to calculate one key from the other. Therefore, the private key cannot be compromised through knowledge of the associated public key.

- Each key in the key pair performs the inverse function of the other. What one key does, only the other can undo. The private key is used for signing and decrypting a message or a document while the public key is used to verify or encrypt.

The primary function of a PKI is to allow the distribution and use of public keys and certificates with security and integrity. E-Lock Digital Signature products and solutions leverage the underlying PKI infrastructure to provide signing and encryption for documents and transactions. While the PKI deals with creation of key pairs and issue and management of digital certificates, digital signature technology deals with use of these keys for various security functions from within the applications.

Digitally signing document

(i) Digital signatures V/S Ink signatures

Before, signing any document, we have to decide to do ink signature or digital signature. However, ink signature are replicated from one document to another by copying the image manually or digitally, but to have credible signature copies, needs some scrutiny and to produce ink signature copies, professional scrutiny is difficult.

On the other hand digital signatures cryptographically bind an electronic identity to an electronic document and digital signature can't be copied. These signatures can be applied to an entire document with tampering on the last page and data on any of the pages can't be altered, while this can also be achieved by signing with ink and numbering all pages of the document.

(ii) Added the signature to the document

The hash result and the user's digital certificate that includes user's Public Key are mixed into a digital signature; it is done by using the user's Private Key to encrypt the document hash. The resulting signature is unique to both the document and the user. Finally, the digital signature is embedded to the document.

If "A" sends the signed document to "B" and "A" use public key (which is included in the signature within the Digital Certificate to authenticate "A" 's signature and to ensure the document didn't alter, after it was signed. Then :

(a) Document validation process starts

(b) Decrypts "A" 's digital signature with his Public Key and gets sent document.

(c) Compares "A" 's document hash with "A" calculated; has – "A" calculates the document hash of the received document and compares it with the hash document in the digital signature. If both hashes are same, the signed document has not been altered. It is presented in Figure-3.

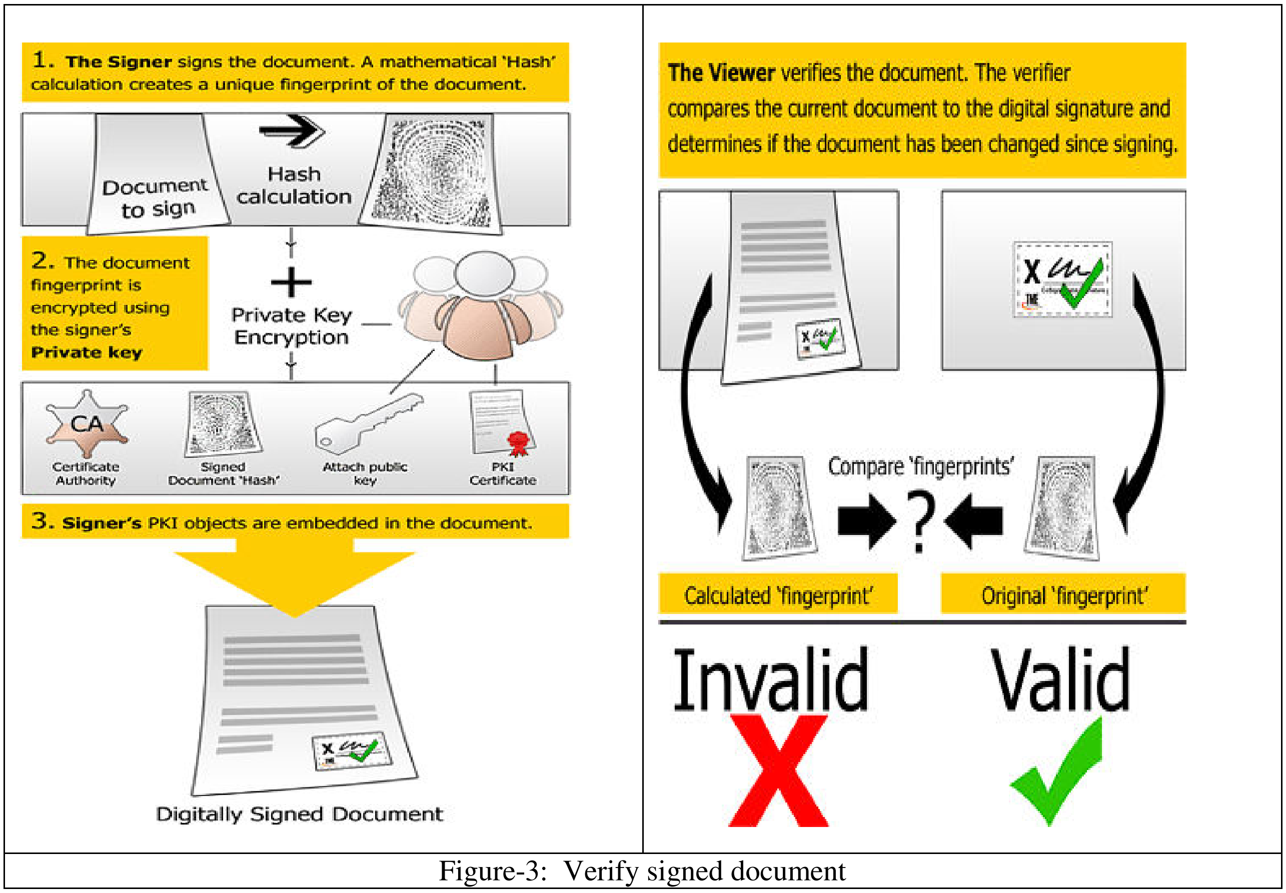

1. The Signer signs the document. A mathematical 'Hash' calculation creates a unique fingerprint of the document.
Document to sign
Hash calculation
2. The document fingerprint is encrypted using the signer's Private key
Private Key Encryption
CA
Certificate Authority
Signed Document 'Hash'
Attach public key
PKI Certificate
3. Signer's PKI objects are embedded in the document.
Digitally Signed Document
The Viewer verifies the document. The verifier compares the current document to the digital signature and determines if the document has been changed since signing.
Compare 'fingerprints'
?
Calculated 'fingerprint'
Original 'fingerprint'
Invalid
Valid

Figure-3: Verify signed document

Source: (Anonymous (2017)

(iii) Application of digital signature

Now a day's majority of organizations believe to speed up of paperless documents with ink signatures or authenticity stamps, where digital signatures support the idea of faster and secure communication / transaction with the evidence to provenance, identity and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The reasons for applying a digital signature for communications are:

(a) Digital signature for secure e-transactions

The shifting from paper-based transactions to paperless transactions (e-transactions) is very easy, fast and economical, but real challenge is to carry out these transactions in a secure and authentic way. For these challenge, digital signature technology is seen as a mechanism to maintain security and authenticity of such transactions for making them simpler and faster. The use of digital signatures not only brings the commercial advantages, but helps to have better environment for the society (Anonymous, 2017, b).

(b) Digital signature for form- 16

The preparation and issuance of employees' Form 16s is a cumbersome task at the end of every financial year for each organization. Traditionally, these forms have been signed and delivered manually and whole process is time consuming, expensive, and cumbersome. Additionally, there are increased possibilities of getting these forms lost, or misplaced, resulting in re-issuance. The re-issuance of Form 16s again; has to undergo with the same process, which is time-consuming.

Looking towards present scenario, any organization can't afford to waste time, manpower and paper on such processes. If a organization going for online with most of these process, manual signing of Form 16s still looks like resource wastage. Therefore, the concept of digitally signing Form 16s is gaining momentum, allowing organizations to save time, money and manpower.

In case of digitally signing of Form 16s, the Indian Information Technology Act 2000 recognizes the use of 'Digital Signatures' as equivalent to 'Physical Signatures'. Therefore, a digitally signed Form 16 has the same legal validity as a physically signed one. Besides, as per Circular No. 2/2007 dated 21/5/2007 from the Income Tax Dept, "The Central Board of Direct Taxes have, therefore, in exercise of powers under section 119 of the Income-tax Act, 1961, decided for the proper administration of this Act to allow the tax payers / deductors, at their option with respect to tax to be deducted at source from income chargeable under the head 'Salaries' to use their digital signatures to authenticate the certificates of deduction of tax at source in Form 16." It is an ideal example for digital signature of Form 16 for organizations to save money and time, without compromising on security and authenticity of the process.

(d) Digital signature for internet banking

Internet banking is also another area for application of digital signature technology, where customer as well as banks can save time, money and other resources. The work will be speedup and faster, which ultimately will improve the efficiency and will helps to reduce the operational cost.

Legal aspects of digital signature

The legal aspects of digital signatures has changed the mind set of people for e-commerce globally, due to the popular applications of digital signature for e-banking, e-tendering, e-procurement, e-approvals, etc. and wagon of e-commerce is reaching new milestones everyday with the help of legal aspects of digital signatures. Further, it is stated that assured authentication and non-repudiation, digital signature technology maintaining integrity and confidentiality of digitally signed electronic documents.

In this direction, several countries came up with their laws, assigning legal validity to digital signatures. Considering the security aspects; digital signatures also helps in paperless businesses. Therefore, many countries are promoting the use of digital signatures, and are making their use mandatory for areas deal with sensitive data (Anonymous, 2017a).

Now a days, use of Internet to reap maximum business benefits with the application of digital signatures is helping them in generating pace and profits within their business, where different countries have laid out certain legal standards to promote digital signatures. Some of these regulations applied across the world to encourage e-transactions (Anonymous, 2017a) are as follows :

- E-SIGN Act (Electronic Signature in Global and National Commerce Act)
- UETA (Uniform Electronic Commerce Act)
- GPEA (Government Paperwork Elimination Act)
- EU law (EU Directive for Electronic Signatures)
- US DoD JITC (Joint Interoperability Test Command)
- Health Insurance Portability and Accountability Act (HIPAA)
- SOX (Sarbanes-Oxley Act)
- 21 CFR Part 11
- Indian IT Act 2000

To make this technology more popular to save time and resources, for better social and business environment, emphasis shall be given to established proper ground, where digital signatures, worldwide legislations have fueled their acceptance in every possible business, from banking to insurance, health care to retail; common consensus is moving towards digitally signed electronic documents, saving time, money, and paper.

(i) Banking, financial services and insurance

The digital signing of any electronic documents is a very responsible action, where once a person has signed any document; he/she cannot repudiate from that responsibility. As main concept behind the digital signatures is non-repudiation and authentication of person signing the document. Hence, a person digitally signing any document/s needs to be very attentive about the contents of signing the document.

(ii) Digital signature technology emerging necessary for society

The application of digital signature helps the individual or company to signing number of papers / documents daily by this chore of activity, which could be very easy, where thousands of employees are working together, if applied digital signature. This is the most efficient way for companies having legal digital signatures binding.

Verification of digital signature

Certificate Authority issued certificates to ensure the validity of the signatories. If, certificates are similar, then you have to identify a user in the system you check his certificate. This certificate issued in registration process once all require information filled in the respective form. However, Digital Signature Certificate is a secure digital key that certifies the identity of the account holder, issued by a Certifying Authority. It contains the identity (name, email, country, APNIC account name and your public key) of the person / account holder/s. Digital Certificates use Public Key Infrastructure, means data that has been digitally signed (encrypted) by a private key, can only be decrypted by its corresponding public key.

Thus, digital signature can be used to authenticate the source of messages. If ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. It is most important for the organizations required electronic signatures at every step of any business process, which required sequential approval in the form of electronic signatures in hierarchical order, depending on the authorities involved in the process. Many times these approving authorities need to add their remarks as well along with their electronic signatures.

Conclusion

Digital signature or e-signature is an ideal tool for the people involved in the process of managing their business. It helps to everyone involved in either e-banking or e-tendering or e-procurement or e-approvals, etc. or any relevant activities of e-commerce, will helps in reducing cost, saving time and utilization of resources more efficiently. It will prove a milestone for people involved in any business / administration or planning of the state / region / country / world.

References

[1] Anonymous (2016) Digital Signature. Web-site: https://en.wikipedia.org/wiki/Digital_signature

[2] Anonymous (2017) Intro to Digital Signatures, web-site : http://www.securedsigning.com/resources/intro-to-digital-signatures; web-site accessed on 10-06-2017

[3] Anonymous (2017,a) Legal Validity Promoting Use of Digital Signatures, web-site : http://www.elock.com/legal-validity-promoting-use-of-digital-signatures.php, web-site accessed on 10-08-2017

[4] Anonymous (2017,b) Digital signature solutions for secure e-transactions.
Web-site: http://www.elock.com/digital-signature-for-secure-e-transactions.php web-site accessed on 10-08-2017

[5] Margaret Rouse and Michael Cobb (2014) Digital Signature.
web-site; http://searchsecurity.techtarget.com/definition/digital-signature; site visited on 10-06-2017