Research Paper

Volume : 4 | Issue : 1 | January 2015 • ISSN No 2277 - 8179

Role of Digital Signature for Authentication of E-Documents

Commerce

KEYWORDS : Cryptography, Digital Signature(DS), DSA, Private and Public Key

Prof. Anil P. Gaikwad PDVVPF's IBMRD Vilad Ghat Ahmednagar (Mahrashtra)

ABSTRACT

Electronic (digital) information handled by information communication technologies such as mobiles, networks etc. Digital signature is a tool to implement cryptography. Digital signature is created by cryptography method using DSA (Digital Signature Algorithm). Digital Signature provides security for E-transaction by using private and public key. Digital signature provides confidentiality, authenticity, non-repudiation, to electronic document. It allows the use of internet for use of internet for carrying out safe and secure E-governance and E-commerce. Digital signature is replaces the traditional method of paper document with the E-document.

Introduction:

With revolution of digital data storage and communication-technologies, digital information can be easily stored, copied, changed and transported. These different properties are very useful as well as having some security issues such as unauthorised access, stealing of data etc.ICT also provides some softwares and date which must kept secure and protected from unauthrised user. The traditional signature systems are not able to change these situations because they are included in the document itself as the part of document. By signing document digitally it is possible to get solution of all these security issues.

The new invented technologies for higher education such as ICT, mobile, virtualization, and network devices are expanding our network and eliminating traditional way of teaching and knowledge gaining. The digital signature security framework allows us to provide strong authentication, repudiation to electronic document. In the digitally signing document we send signature as separate document. As a result digital signatures are poised to enter as a primary vehicle for establishing trust for a wide variety of electronic transaction.

Digital signatures are formed under digital signature standard (DSS).It is not the digital image version of hand written signature .It is something like electronic stamp digital signature is an alphabetic string obtained through processing the transmitted text by a hash function the purpose of this mathematical hash function is to verify the source text and confirm whether the text is undergoing changes. Digital signatures is generated and processed by cryptographic technology and its security depends on security level of the cryptosystem. Hence using digital signature it is possible to keep security level higher than the handwritten signature especially for information on network. The digital signature is generated using private key.

For the use of digital signature the recipient receives the message and signature. The recipients need to apply a verification technique to the combination of message and the signature. To verify authenticity digital signatures ensures privacy of data and prevent it from unauthorised data accesses. Because of all its characteristics digital signatures are added and apply in many areas like E-banking, E-government, E-tendering, health, medicines etc.

-Health care and pharmacy organisation for protection of patient's digital medical records and prescription given by expert in the field.

-Banking and financial services and insurance requires processes, accuracy and security.

-Government: In E-government program all administrative agencies , courts, various government departments adapted digital signature to streamline their process, improve efficiency, reduces cost and time, secure and manage data.

-Other industries like telecom, IT, retail, defence, manufacturing etc. are implementing electronic signature solution for E-invoking and E-tendering.

This paper is organised as follow:

Section1-Abstract and Introduction

Section2-Keyfactors such as privacy, authenticity, confidentiality, cryptography, non-repudiation

Section3-Digital signature algorithm

Section4-Introduces features of digital signature

Section5-Describes conclusion that how paper documents are replaced with the E-document (digital signature) in authenticand secure management.

Key factors of Digital Signature:

Cryptography: cryptography is the science of information security. Cryptography includes techniques such as microdots, merging word with the images and other way to hide information in storage or transit. However in today's computer centric world, cryptography is most often associated with scrambling plaintext into cipher text called encryption, then back again to plaintext known as description.

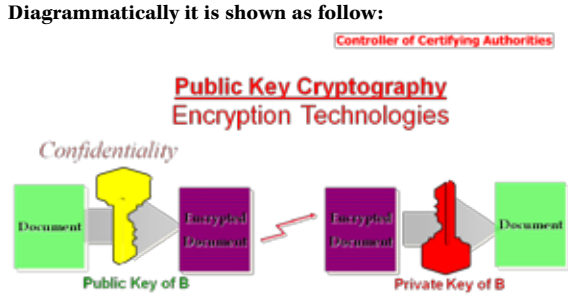
There are two main types of cryptography:

-secret key cryptography
-public key cryptography

In cryptography the term key refers to a numeric value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

Messages are encrypted by the sender using the key and decrypted by the receiver by using the same key.

Diagrammatically it is shown as follow:



This method works well if you are communicating with a limited number of people, but it comes impractical to exchange the secret key with the large number of people.

The public key can be freely distributed without compromising

the private key, which must be kept secrets by its owner. Because these key works only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key.

2) Confidentiality:
Data confidentiality refers to a situation in which a message is inaccessible to others except the intended recipient. Encryption and decryption ensure confidentiality.

3) Authenticity:
Authentication means verifying the identity of entities that the person with whom you are corresponding are actually the same who they say they are. This is achieved by public and private key generation.

4) Integrity:
Integrity means ensuring that data can not be corrupted or modified or transaction is unaltered. This can be verified using message digest to message which is transmitted from sender to receiver.

5) Non-repudiation:
It provides security against denial by third unauthorised party which involved in communication. This is provided through public key cryptography by digital signing the document.

Features of Digital signature:
-DS are easily transportable and can not be imitated by someone others

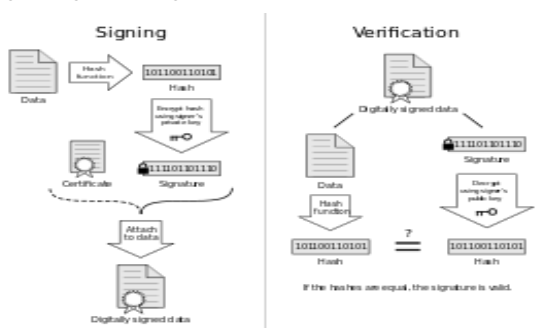
-A DS contains all the significances of conventional signature plus a few more practical and sensitive features for secure email and credit card transaction.

-The DS must use some information that is unique to sender, easy to produce, easy to recognize and verify authenticity.

-A DS is an encrypted version of a message digest, attatched together with a message.

-The basis of digital signature is public key cryptography which is the most fundamental invention and development of modern cryptography.

Digital Signature Algorithm:



Conclusion:
In this paper we have been able to verify why the paper documents are getting replaced with the E-document.

Digital signature provides public and private keys and so files encrypted with the public key can only be decrypted by the holder of the private key.

Apart from the security advantages, this system has been proved to maintain the integrity of the information secured. The system has therefore eliminated the fear of losing vital information.

Cryptography is important for more than just privacy, however. Cryptography protects the world's banking system as well. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and steal the money without trace. Similarly it is also useful in ICT based education for reliable knowledge, authentic personality and protect from misguided information.

REFERENCE

1) Prakash Kuppuswami, peer mohmmad appa, dr.saeed Q. Y. Al khalidi, "A new efficient digital signature scheme algorithm based on Block cipher" IOSR journal of computer engineering ISSN: 2278-0661,ISBN: 2278-8727 vol.7, pp47-52, nov-dec2012. | 2) Neetesh sexena and Narendra S. Chaudhary "secure Encryption with the digital signature Approach for short message services" IEEE, 2012 | 3) Kaur Ranveer and Amandeep Kaur, "Digital Signature" IEEE2012 Int. conf on Computing Science, 2012 | 4) Junling Zhang "A study on Application of digital Signature Technology" int Conf.On Networking and Digital society, IEEE 2010. | 5) Guidelines for usage of Digital Signature in E-governance version1.0,Dec 2010. | 6) S.R.Subhramanya and Byung K.YI, "Digital Signature" | IEEE POTENTIALS, pp.5-8, April 2006. | 7) Tanembaum A.S.Computer Networks(2003), 4th Edition, pp.722-762,2003 | 8) William Stalling, Cryptography and network security | (2002), 3rd Edition, 2002. |