ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

DIGITAL SIGNATURES

Neetika Devi[1], Inderjit Kaur[2]

Assistant Professor, Department Of Commerce, MRPD Government College, Talwara (District Hoshiarpur)[1]

Assistant Professor, Department Of Computer Science, MRPD Government College, Talwara (District Hoshiarpur)[2]

Abstract: A Digital Signature is an important tool of cyber security. It is just like a handwritten signature. Digital signatures are most secure type of signatures. Digital signatures are commonly used for software distribution, financial transaction, contract management software etc. A Digital Signature scheme has three algorithms-A key generation algorithm, A signing algorithm and A signature verifying algorithm. In Digital signatures, A document is signed electronically and it validates the signer. It authenticates the document from the sender and ensures the unalteration of document in transit. This paper is an attempt to throw a light on Digital Signatures and its uses and purposes in different segments. This paper also shows the working of digital signatures.

Key Words: Digital Signatures, Public Key Infrastructure technology, Encryption, Security.

1. INTRODUCTION

A Digital signature authenticates digital messages. It is a mathematical scheme which has features like Authentication, non-repudiation and integrity. If any digital document carries digital signature, it gives a recipient reason to believe that message was created by a known sender, hence it authenticates the digital document. Digital signatures deploy the Public Key Infrastructure (PKI) technology. A sender cannot deny his identity once he signs his document electronically. Digital Signatures are just like handwritten signatures. It is a data attached to any digital message. There is an Integrity in Digital Signature. It means that message is not altered in transit.

Digital Signatures enable the Authentication, on-repudiation and Integrity of digital messages. A digital signature certificate is normally valid for 1 or 2 years, after which it can be reviewed. Digital signatures cannot be forged. Certification Agency (CA) issues Digital Signature. A Digital signature is signed with the CA's private key.

There is a legal recognisation provided to digital signatures by Information Technology Act 2000. The digital signatures are now accepted in any Indian court of law like handwritten signatures. Digital Signature Certificate is issued by a Licensing Certifying Authority in India. Directors, Auditors, Company Secretary, Bank Officials and Other Authorised Signatories have to obtain Digital Signature Certificate. Users can browse and attach the digital signature at the time of submission of the required document.

Digital Signatures should be obtained from Certifying Authorities (CA) in India. CA must check information carefully before issuing a digital certificate.

A Digital Signature scheme has three algorithms-A key generation algorithm, A signing algorithm and A signature verifying algorithm

- A key generation algorithm selects a private key from a set of possible private keys.
- A signing algorithm produces a signature.
- A signature verifying algorithm either accepts or rejects the message's claim to authenticity.

2. Review of Literature

Researchers, Abhishek Roy and Sunil Karforma in their Research paper titled "A survey on digital signatures and its applications" have made a thorough study of the industry standard digital signature schemes to obtain optimum security level for the electronic mechanisms and explored its probable applications in various domains. The success rate of various electronic mechanisms such as E-Governance, E-Learning, E-Shopping, E-Voting etc. depends upon the

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

security, authenticity and integrity of the information that is being transmitted between the sender and the receiver.

Researchers, Hongjie Zhu and Daxing Li, in their Research paper titled "Research on Digital Signatures in Electronic Commerce" proposed a kind of digital signature based on public key and a material digital signature system is given with Java index terms-Electronic commerce. Public confidence is important in E-commerce building and using. It comes from the information safety and the valid protection to privacy. The main aim of the text is to apply digital signatures technology in E-commerce system, provide solution to the safety problems and prevent all kinds of potential safety hazards.

3. Digital Signatures- Its Uses and Purposes

A Digital Signature Certificate is recognised by the legal system. Digital Signature Certificates are used for many purposes

- to Sign documents or transactions
- to secure authentication
- to avoid the risk of forged payments
- to resolve dispute between sender and receiver as there is non-repudiation in its features.

A. Uses of Digital Signatures

- To verify the persons signed electronic documents or e-mails.
- To access websites
- To sign mails digitally
- Total transparency through e-Governance
- Provides Customer focused approach
- Provides service level fulfillment
- Helpful in e-filing such as e-returns. Filing of e-returns requires digital signatures but it is not mandatory. Helpful in filing tax returns in a very convenient and secure way
- Used to prove ownership of a domain name and establish SSL/TLS encrypted secured sessions between the company website and the user for web based transactions.
- Authenticates the identity of the user electronically.
- Provides a high level of security for various online transactions because there is privacy of the information exchanged using a digital signature.
- Digital signatures have made the tendering process very convenient and transparent. A Digital signature Certificate is essential for companies that take part in e-tendering processes on various government sites.
- A Digital Signature Certificate is very essential for all e-Procurement processes.
- Digital signatures help in overcoming geographical limitations as there is no need to send the document physically if it is digitally signed.
- Digital Signatures help in keeping pace with present technology.
- A Digital Signature Certificate is very much useful in Foreign Trade.EXIM organisations should have DSC, as DGFT asks for it to process the documents for issuing license. Digital Signatures are helpful in preventing fraudulent practices such as identity thefts.

A Class-3 Digital Signature is essential for any organisation seeking an Import or Export license.

B. Types of Digital Signatures

There are basically three types of Digital Signature Certificates (DSC).
Class-1
Class-2
Class-3
These all have different levels of security. Class-2 DSCs are used by all the authorised signatories of companies under MCA21 and by CA/CS/CWA and Tax Practioners under MCA21.
Class-3 DSCs are used by companies filing e-tender, stock broking companies for signing contract notes, websites having live I.P etc.

4. Working of Digital Signatures

A Digital Signature Certificate is a very strong tool of Cyber Security. A pair of asymmetric keys is used. These keys are-

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

Public Key and Private Key. DSC uses a very complex algorithm to generate these keys.

Private Key is held securely by the user and Public Key is available publicly. To create a Digital Signature, Private Key hashes the content of the document (hash function) and uses the private information of the user to sign the document and Hence document is encrypted at the signer's end.

Hash function is a mathematical calculation that gives the message a hash value. The sender of a message completes this calculation by hash function and then digital signature is appended to the document. Then message encrypted with the sender's private key is sent to the destination along with the signature.

The receiver decrypts the signature using the sender's public key and if result matches with the copy of the message received, the receiver can be sure about the original identity of the sender.

A. Digital Signatures and Cyber Security

Digital Signatures provide protection again hacking. Content of the document cannot be altered in transit. This ensures integrity and confidentiality of the content. There are no man-in-the-middle attacks.

B. Securing Channels of Communication

The Public key encryption concept is used for securing channels of communication. Channels of communication are secured through Secure Sockets Layer(SSL), Secure Hypertext Transfer Protocol(S-HTTP) and Virtual Private Network(VPNs).So, Communication is protected by Public key encryption.

C. Protecting the Network

After protecting the communication, next step is to protect the network, the servers and the clients on the network. Firewalls filter communication packets and use rules to inspect network packets. Firewalls filter the incoming and outgoing traffic that flows through a system. They can allow or block the traffic. So firewalls enhance the security of a network.

A Proxy server is a computer application that functions as an intermediary between a web browser and the internet. Proxy servers help in improving web performance by storing a copy of frequently used WebPages. Proxy server provides WebPages to the browser from its collection on the request of browser. It is faster than going to the web.

Proxy servers improve security by filtering out some web content and malicious software. Proxy servers are used mostly by networks in organisations and companies. Typically, people connecting to the internet from home will not use a proxy server.

D. RSA encryption in Digital Certificates

Most systems now use RSA encryption. It is based on Public Key Cryptography. This signature method verifies the identity of sender. It also verifies that the original contents of the message have not been altered in anyway. This authentication is even better than a signature on a paper. This type of Digital signature cannot be forged.

5. Conclusion

Digital signatures are proving very helpful in today's digital age. They are very efficient and secure. Digital signatures are ideal for both small and large organizations. Digital signatures ensure better workflow efficiency and they are also helpful in reducing waste and being environmental friendly. Digital signatures are becoming more and more important for electronic commerce security because of its authenticity, data integrity protecting and privacy.

References:

1. https://en.wikipedia.org/wiki/Digital_signature
2. https://www.emptrust.com/blog/benefits-of-using-digital-signatures
3. https://www.researchgate.net/publication/233391380_A_survey_on_digital_signatures_and_its_applications
4. http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp807-809.pdf
5. E-Commerce , Sandeep K.Bansal, Sanjeev K.Bansal, Rama Bansal,Kalyani Publishers.
6. E-Commerce , Suman Dhull, Minakshi Bhardwaj, Kalyani Publishers.

BIOGRAPHY

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 10, March 2018

First Author Neetika Devi is an Assistant Prof. in MRPD Govt college Talwara. She is from Department of Commerce. She has done M.Com and M.Phil. She is UGC-NET Qualified. She is pursuing Ph.D. in commerce. Her papers are published in various journals. She has keen interest in research. She keeps visiting seminars and conferences.

Second Author Inderjit Kaur is an Assistant Professor in MRPD Govt College Talwara. She is from Department of Computer Sciences. She has done PGDCA, MSC IT and MCA. She has keen interest in research area.