International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

STUDY ON SERVICES PROVIDED BY DIGITAL SIGNATURES IN E -COMMERCE

Yachana Shantaram Rane

Student, Dept. of MCA, YMT College Of Management-Kharghar Navi Mumbai ,Maharashtra.

Abstract - *The digital signature is been generated for the purpose of transmitting the actual data without any changes or alteration. The digital Signature Service may operate as Web Server Application on the clients or users system. The client can send document to the sever as well as receive back the same document or vice-versa. The DSS (Digital Signature Services) Core specifications grant the basic protocols and elements which are adapted to base the specific use cases in the DSS profiles. The study is been done in the of electronic commerce field (e-commerce"), and specifically for Digital Signature been used in the field of E-commerce. Some researchers have already started researching on digital signature is to ensure integrity of the message as it helps in verifying whether actual messages is been transmitted or not the integrity factor helps in verifying the accuracy of the message that is been exchanged between the two parties via unsecured modes like the Internet.*

Key Words: **Signature Services, E-Commerce, CA's, Privacy and Security, Tools.**

1.INTRODUCTION

Electronic commerce called as 'E-Commerce' has occurred a extremely high popularity in today's life due to high use of Internet.[3] Generally E-Commerce is transaction taking place between two parties. Lets take an example, of an electronic transaction is made among the customer and an online bank person or a transaction between a company and its partners. E-Commerce plays a very important role in this. The transaction done should be safe there should not be able to make any changes. The most importantly it should be secure enough so that fraud factor should be decreased.[3] The main function that is the integrity and authenticity is been provided to secure the transactions. .The security function arises not only from the process of encryption to create a digital signature but also from the role of a CA to verify the identity of a party. The CA helps in verifying whether the party accessing the transactions is real or fake one.

2. DIGITAL SIGNATURE AND ITS WORKING

The sender uses a signing algorithm to apply on the given message. The message and the signature are sent to the receiver.[8] When the receiver receives the message and the signature it applies the verifying algorithm to the check for the result that is occurred . If the result been obtained is accurate and correct, the message is accepted; otherwise, it is rejected. The Digital Signal uses the private key encryption and public key encryption methods. This is how the working of Digital Signature takes place. There are various services that are been provided Digital signature can be used in all electronic communications.[1] It is an electronic stamp or electronic content that append to the document. As it ensure the document is not been changed or altered during transmission process.[2] A Digital Signature is a process used for signing an electronic document with all the security been provided.

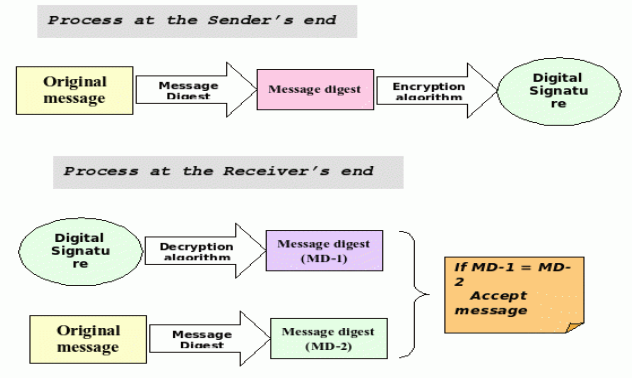

Fig -1: Digital Signature – Process at Sender's and Receiver's End

Working Of Diagram:[8]

a. On the sending side, the sender would encrypt the message digest with her private key that is been known to her. The sender must secretly hold the private key constantly.

b. The output of this process which is been obtained is called as the digital signature for this specific and actual message.

c. The sender sends the original message along with the digital signature to the receiver at another end.

d. The receiver verifies (decrypts) the digital signature using the sender's public key, which is available very freely. This should provide the receiver a message digest stating MD-1.

e. The receiver also computes a fresh message digest on the original message, stating MD-2.

If MD-1 = MD-2, we achieve both message integrity (in which message has not been doctored as long as the attacker is unable to know the sender's private key) and non-repudiation (the message is proven to be sent by the sender, for the reason that only she knows the private key corresponding to this public key).[8]

Digital signatures are maintaining three important functions:

This is the very important three functions that the Digital Signature follows and endows [7]

Authentication – This function helps to authenticate the identity of the person who signed the data so it is known who have reciprocated in the transaction. A digital signature give recipient reason to believe the message was been created by the known sender so that later on the sender cannot deny having the send message.

Integrity–This function helps to protect the integrity of the data so it is possible to know the message read has not been transit or altered, either accidentally or maliciously by someone.

Non-repudiation– This function is to allow it to be proved later who interacted in a transaction about the data been send and received. Typically this function refers to ability that party or the communication cannot deny the authenticity of their own signature that they originated.

3. E-COMMERCE IN DIGITAL SIGNATURE

In general form, e-commerce involves electronic transactions or communication that takes between two or more than two parties. For example, an E-commerce transaction may be between a consumer and a non-line merchant, or an e-commerce transaction may be implemented for buying goods and services between a company and its dealer or the retailer. Regardless of the nature of the transaction, the most important thing in order to promote the use of e-commerce, there is a demand for the major security that is, secure transactions must been taken place among the parties exchanging electronic transactions.

A secure transaction involves both the ability to authenticate and check that information that is been transmitted as part of the transaction, has not been transformed or corrected, as well as the ability to authenticate the parties among themselves that is mutual authentication at the same time. In order to provide secure transactions for use in e-commerce, digital Signatures have been used. A digital signature is generally an encrypted electronic fingerprint. Then this encrypted fingerprint is attached to a document, the digital signature signs that the owner issued on the document. This feature of digital signatures enables the conduction of e-commerce to occur in a legal manner. The process of generating a digital signature involves the use of both the document a certificate, particular to each individual for efficiency and compatibility, along with signature, that constitutes a unique fingerprint taken of the individual on that document.

4. CERTIFICATION AUTHORITIES IN DIGITAL SIGNATURE

The authentication process is simply based on the fact that the public key been used is actually belonging to the proper or authenticated user or signer.[6] There is a risk which exists that anyone else can create the same key pair, and can also place the same public key by some other name. This can help the fake key pair to signs the actual electronic message.

The public key and the private key pair have no idea with the identity it just simply pair and try to match the numbers. This give rise to the question that the assurance should exist that the public key is really belonging to the actual claimed identity.[6]The answer is depended upon the third party to certify these public keys. The third party can make a decision between the identity and the public key. These third parties are called as 'Certification Authorities' (CA's) and this are accepted by all the users and there is also 'Trusted Third Party' (TTT). This provide a very much high level of security using the registered Digital Signature been used to sign the electronic messages. This is so much trusted that it becomes similar to notary public to manually sign

The CA is able to check the identity of the use for example passing out the certificates. This type of assurance is been provide by the CA. Other certificates are been issued after receiving third party proofing like personal information been provided during the process. Credit cards on other hand offer security [5]. There is balance struck between privacy and security with the mean of payment. Privacy is been provided with security in hand in hand.

5. SECURITY AND PRIVACY

When customers conduct their private transactions there is chances that personal information been filled during registration is been revealed to others and misuse of that information can be done easily.[5]. It's very much important that the transaction taking place should be secure. When the transaction is secure and safe it is through

be protected by corruption also.[6]. There are many technologies including cryptographic techniques that can migrate the vulnerabilities. In this phase privacy is the ability to not be able to reveal the identity of the user and also the confidential data during the transaction

PURPOSE OF SECURITY [5]

1. Data Confidentiality –It is provided by encryption /decryption method whether the information stored in the system is been secured and is protected against unauthorized one's.

2. Authentication and Identification – It helps in verifying the identity of the user, through they can use specific credentials such as passwords, locks, token etc. It helps in ensuring that someone is who he or she retrieves data to be is implemented with digital signatures.

3. Access Control –It governs what resources a user may access on the system. That is permission to access a particular resource. Proper IDs and password are needed to be used .Lock and IDs are two mechanisms of access control

E-COMMERCE SECURITY TOOLS [5]

1. Firewall - Its use to protect the hardware and the software of the system. It is been designed to prevent unauthorized access from private network.

2. Public Key infrastructure - It is series of processes for the association of cryptographic key. It is good practices for secure communication between the parties.

3. Encryption software-This software is been used for establishing the identity of the user. It helps in protecting the data at simplest level so that other people can't read it only authorized person should have the access.

4. Digital certificates- This certificate allows the user to exchange the information securely among each other over internet using public key infrastructure.

5. Digital Signatures -As the contracts are paperless in e-commerce digital signature helps in making contractual agreement.

6. Biometrics - Biometrics helps in identifying people based on unique physical characteristics like retinal scan, fingerprints, voice

7. Passwords- It is a security measure been taken handled by the system that can due protect users transaction from hacker

8. Locks and bars- This are in the network operations centers.

6. CONCLUSION

From Internet and E-commerce have the possibilities for endless business and customers services. Digital Signatures is therefore essential to promote E-Commerce as studied in paper.

Digital signatures are the standard element used for software distribution along with E-Commerce transactions. In future Digital Signature will be getting more scope with more security features to be added according to the study. Identity based digital signatures and the associated Certification Authorities have little immediate relevance in the development of Electronic Commerce. Digital Signature have became equivalent to handwritten signatures and stamped seals.

Digital Signature has become more secure to detect forgery as nowadays fraud had increased during the transactions.

7. REFERENCES

1. Secure wireless electronic-commerce system with digital product certificates and digital license certificates
Publication number US6223291 B1
Inventors Larry C. Puhl, Dean H. Vogler, Ezzat A. Dabbish

2. A Digital Signature Based on Conventional Encryption Functions
By Ralph C. Merkle Elxsidy Place San Jose, CA 95131
Inventors: Larry C. Puhl, West Dundee; Dean H. *
Cited b examiner Vogler, Algonquin; Ezzat A. Dabbish
Patent N0.: US 6,223,291 B1

3 . DIGITAL SIGNATURE SERVICE W0 WO 99/22486 5/1999
W0 WO 99/48243 9/1999
(75) Inventors: Tony F. Kinnis, Murray

4. PKI Implementing and managing E- security, Mcgraw-hill , 2001(Andrew nash, William duane ,Celia joseph, Derek brink

5.The study of E-Commerce Security Issues and Solutions
Niranjanamurthy M 1, DR. Dharmendra Chahar 2
Research Scholar, Dept. of MCA, MSRIT, Bangalore, INDIA1

5.Privacy and Security Issues in E-Commerce
Mark S. Ackerman and Donald T. Davis, Jr.

6.Public key/signature cryptosystem with enhanced digital signature certification
Publication number US5005200 A
Inventors Addison M. Fischer

7.How Does it Work? Digital Signature Technology for Dummies Posted by John Harris

8.Public Key Encryption and Digital Signature: How do they work? [pdf]

9. www.verisign.com

10. www.thawte.com

11.. http://www.indicthreads.com/

12..https://en.wikibooks.org/wiki/Cryp