IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 56-60
www.iosrjournals.org

Digital Signature Certificate: A Great scientific Knowledge for Nation Development

[*]Shaikh Imtiyaj, Er. Ratan kumar Agrawal, Dr A K Hota
Computer Science Engineer-Senior Programmer Level 1, eProcurement Project, Ministry of Elect & IT, NIC, Bhubaneswar, Odisha, India
Chief Engineer cum Chief Manager (Tech), eProcurement Cell, Govt. of Odisha, Bhubaneswar, Odisha, India
Scientist- Senior Technical Director, Ministry of Elect & IT, Bhubaneswar, Odisha, India
Corresponding Author: Shaikh Imtiyaj

Abstract: *Nations of the world are now competing to move progressively towards knowledge based societies as well as economics and science and its offshoot technology are playing significant roles. Information and Communication Technology is being increasingly used in day to day life of a common man and it is rapidly becoming an integral part of providing the better governance services to the citizens of a country. e-Governance aims to provide good governance to the public by using the Information and Communication Technology (ICT) for speedy, accurate, transparent and secured services. E-Governance tries to eliminate the digital divide among urban and rural people. Timely and efficient delivery of e-Governance services is an important aspect. Now a days, departments, business sectors and customers alike collect, store and transmit vast amount of information electronically as they have started believing that their information is secure. The digital signature technique is essential for secure transaction over open networks. Hash functions are the most widespread among all cryptographic primitives and are currently used in multiple cryptographic schemes and security protocols. Digital Signature Certificate (DSC) provides high level of security for online transactions. Digital Signature Certificate is the digital equivalent that can be presented electronically to prove the identity, to access information or services on the Internet or to sign certain documents digitally. Like physical documents are signed manually, electronic documents are required to be signed digitally using a DSC. Digital Signature Certificates provide Authentication, Privacy, Non repudiation and Integrity. You can use certificates to encrypt information such that only the intended recipient can read it. You can digitally sign information to provide assurance to the recipient that it has not been altered in transit, and enable verification that you actually sent the message. In this research paper the study of DSC, implementation of DSC, Message Digest algorithm, DSC work flow and DSC risk is presented. The usage of DSC in applications such as e-Procurement, efiling Income Tax returns, fund transfer in The Mahatma Gandhi National Rural Employment Guarantee Act 2005(Mahatma Gandhi NREGA) Project at all the Gram Panchayats, Blocks, Districts, States levels; Online Counseling, Collectorate Offices, Registration Offices and many more areas is gradually increasing day by day, improving success in carrying out business functions. To enhance the power of security and better implementation further research is in progress. This study focuses on different opportunities of G2B initiatives in India. The basic objective of research is to provide a model for better implementation of e-Governance application.*

Keywords: *Information and Communication Technology, Digital Signature Certificate, e-Governance*

Date of Submission: 20-07-2017 Date of acceptance: 28-07-2017

I. Introduction

Nations of the world are now competing to move progressively towards knowledge based societies as well as economics and science and its offshoot technology are playing significant roles. Information and Communication Technology is being increasingly used in day to day life of a common man and it is rapidly becoming an integral part of providing the better governance services to the citizens of a country. e-Governance aims to provide good governance to the public by using the Information and Communication Technology (ICT) for speedy, accurate, transparent and secured services. e-Governance refers to Government's use of technology particularly web based internet applications to enhance the access to and delivery of government information and services to their citizens, public agencies, employees, business partners, financial institutions and government departments. The Government envisions providing good governance by establishing a Committed, Accountable, Responsive, Inspiring, Nationalist, and Genuine Government - CARING Government. The digital divide among urban and rural people is eliminated to maximum extend by use of e-Governance. Timely and efficient delivery of e-Governance services is an important aspect. Indian IT-Act 2000 has mandated the usage of Digital Signature Certificate (DSC) for e-Governance applications.

1.1 e-Governance: Objective

- Providing information speedily to all citizens
- Improving transparency
- Improving public services such as transportation, power, health, water, security and municipal services etc.
- Reduce Corruption

1.2 e-Governance Development Model

The e-Governance Models are

- G2C : Government to Citizens
- G2B : Government to Business
- G2G : Government to Government

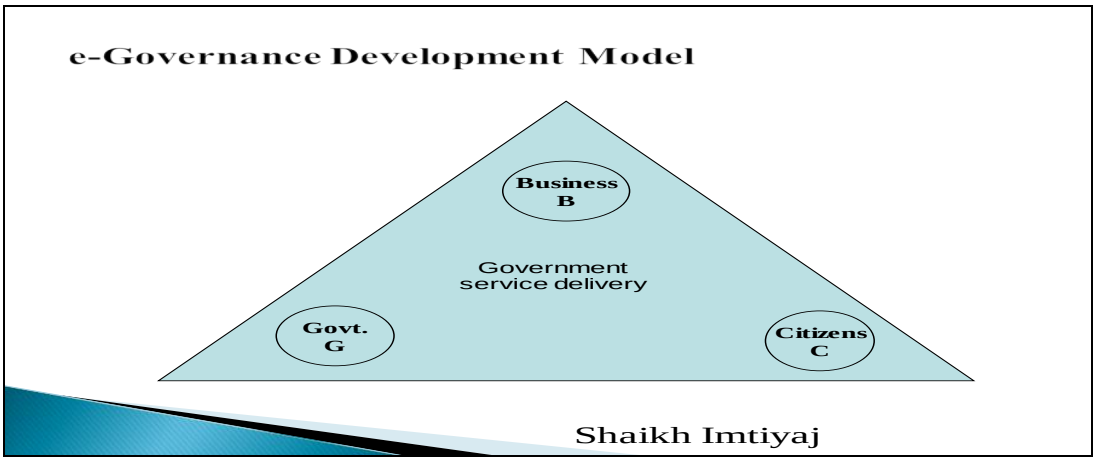

Figure.1- Governance Development Model

II. Digital Signature Certificate (Dsc)

Digital Signature Certificate (DSC) is the digital equivalent that is electronic format of physical or paper certificate. DSC can be presented electronically to prove the identity, to access information or services on the Internet or to sign certain documents digitally. Like physical documents are signed manually, electronic documents are required to be signed digitally using a DSC. Digital Signature Certificates provide Authorization, Authentication, Privacy, Non repudiation and Integrity. IT Act 2000 in Government of India gives legal validity to electronic transactions that are digitally signed. DSC provides high level of security for online transactions. You can use certificates to encrypt information such that only the intended recipient can read it. You can digitally sign information to provide assurance to the recipient that it has not been altered in transit, and enable verification that you actually sent the message.

Figure.2- Digital Signature Certificate (Smart Card / eToken)

2.1 How Digital Signature works

The Digital Signatures require a key pair called the **Private** Key and **Public** key. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like Crypto Smart Card or eToken as above shown in Figure.2. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key. In order to digitally sign an electronic document, the sender uses his/her **Private Key**. In order to verify the digital signature, the recipient uses the sender's **Public Key**.

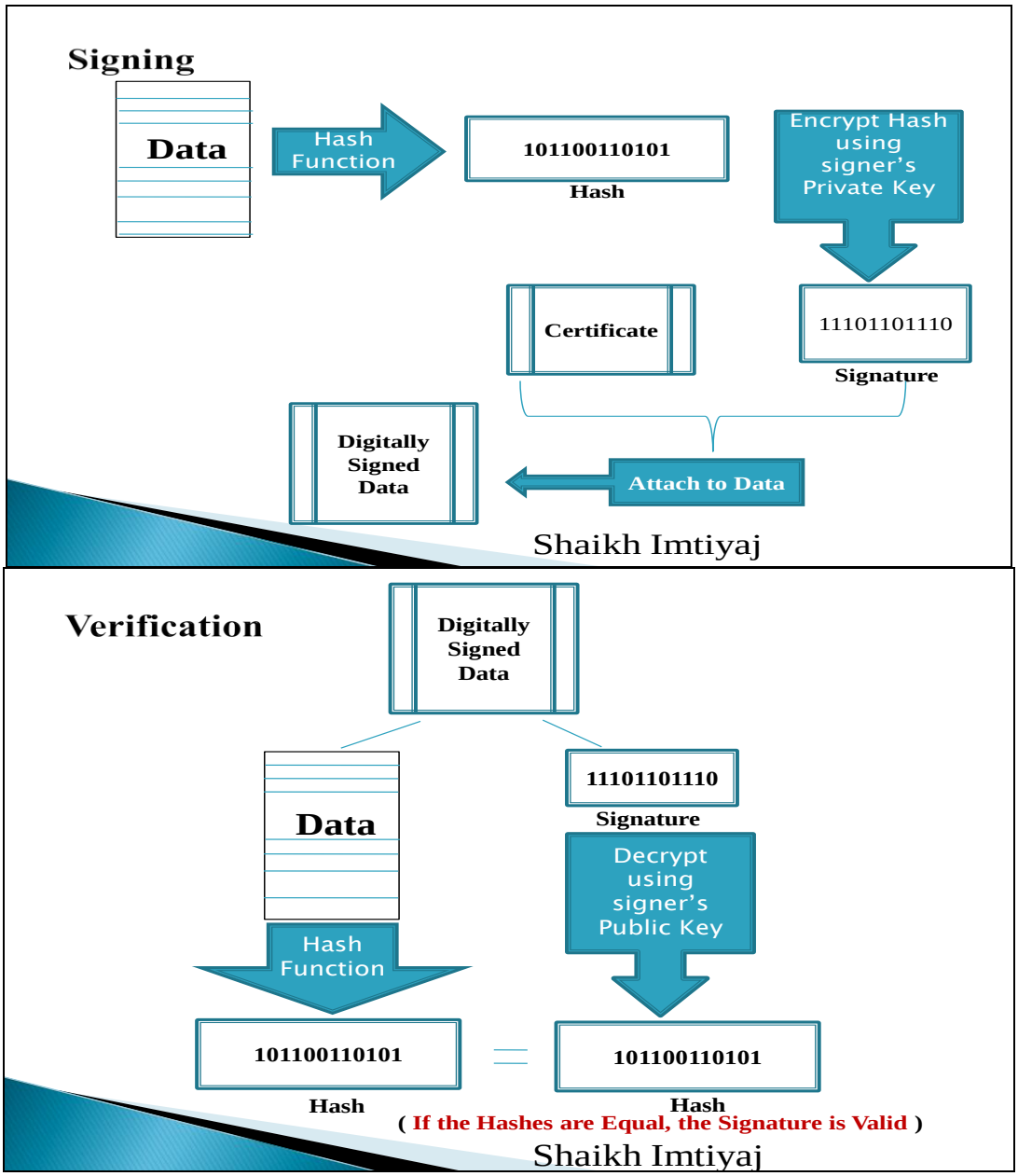

Figure.3- DSC working process

The Hash of a message is also known as Message digest , is a small piece of data that results by applying a particular mathematical calculation (Hashing function) on the message.

III. Algorithm Implementation

DSC is based on MD5 algorithm from Cryptography. MD5 is Message Digest algorithm, which takes as input a message of arbitrary length and produces as output a 128-bit "message digest" of the input. MD5 is more secure than MD4.

IV. Functions Of Digital Signature Certificate (DSC)

1. Signing
2. Encryption/ Decryption

4.1. Classes of Digital Signature Certificate (DSC)

Depending upon requirement of assurance level and usage of DSC, the type of classes are follows:
Class-1 Certificate: provides minimum level of assurance. Intended for personal use. It does no strongly authenticate identity and is therefore not applicable for commercial use.
Class-2 Certificate: provides higher level of assurance confirming the details submitted in the DSC Request Form, including photograph and documentary proof in respect of at least one of the identification details.
Class-3 Certificate: provides highest level of assurances, as verification process is very stringent and applicant has to present himself/herself before the CA.

A Certifying Authority (CA) is authorized by Controller of Certifying Authority (CCA) to issue DSC. Any person may submit an application to the Certifying Authority for issue of the DSC. The applicant holds the private key corresponding to the public key to be listed in the DSC. The applicant holds a private key, which is capable of creating a Digital Signature. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant. It is very important to keep the private key securely. Depending on the usage, the DSC keeps Signing Certificate and/or Encryption Certificate or both.
The Certifying Authorities (CAs) are follows-

(i) NIC
(ii) Safescrypt
(iii) TCS
(iv) MtnlTrusline
(v) GNFC
(vi) E-Mudhra
(vii) IDRBT

4.2 Types of Digital Signature Certificate (DSC)

(i) Signing Certificate

Signing certificates identify a person. This certificate contains the full name and personal particulars of an individual. It is used for signing documents and emails etc.

(ii) Encryption Certificate

Encryption certificates are used to encrypt the message.

(iii) Server Certificate

Server certificates identify a server. Server certificates contain the host name or IP address. It is used for SSL to ensure secure communication of data over the network.

V. Digital Signature Certificate (Dsc) Risk

Figure.4- DSC Risk

VI. Implementation

Sending and receiving digitally signed and encrypted emails
For signing web forms
e-tendering documents
e-Procurement

Voters List Preparation
Registrar of Companies efiling
efiling Income Tax returns
Signing documents like MSWord, MS Excel and PDFs etc.,
Foreign Trade
Employee Provident Fund
Fund transfer in The Mahatma Gandhi National Rural Employment Guarantee Act 2005(Mahatma Gandhi NREGA) Project at all the Gram Panchayats, Blocks, Districts, States levels;
Online Counseling
eDistrict
eOffice
IRCTC
NSDG
DGFT
MCA21
RBI Applications (SFMS)
Establish SSL encrypted secured sessions between website and the user in web based transaction

VII. Conclusion And Future Work

In this research paper the study of DSC, implementation of DSC, Message Digest algorithm, DSC work flow and DSC risk is presented. The usage of DSC and implementation of Message Digest algorithm must be focused to make the e-Governance applications more successful in a developing country like India. Still the usage of DSC is increasing day by day among the citizens for its secure techniques. To enhance the power of security and better implementation further research is in progress. This study focuses on different opportunities of e-Governance initiatives in India. The basic objective of research is to provide a model for better implementation of e-Governance application.

References

[1] Shaikh Imtiyaj, Er. Ratan Kumar Agrawal, Dr. A K Hota "Study of Online Banking Solution for e-Governance initiatives: e-Procurement –A Scientific Knowledge", IOSR Journal of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727,Volume 19,Issue 2,Ver. IV(Mar-Apr. 2017), PP 55-61
[2] Shaikh Imtiyaj, Er. Govinda Chandra Mangual, Dr. A K Hota "Study of e-Governance initiatives: e-Procurement a Business Reform Process for Odisha's Development", IOSR Journal of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727,Volume 18,Issue 6,Ver. 1(Nov-Dec. 2016), PP 44-53
[3] Shaikh Imtiyaj, Er Govinda Chandra Mangual, "An Indepth Understanding of e-Governance initiatives: e-Procurement –A Great Success in Odisha", IOSR Journal of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727,Volume 18,Issue 4,Ver. V(Jul-Aug. 2016), PP 144-147
[4] Shaikh Imtiyaj, N.R Biswal, T.P Ray, Dr A.K Hota, "An Indepth Understanding of e-Procurement : A Case Study Approach", IOSR Journal of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727,Volume 17,Issue 6,Ver. V(Nov-Dec. 2015), PP 20-24
[5] Shaikh Imtiyaj, N.R Biswal, T.P Ray, Dr A.K Hota , "Digital Signature Certificate: A blessing for e-Governance Application in Human Development", International Journal of Advanced Research in Science, Engineering and Technology,Vol. 2, Issue 1 , pp 350-355,January 2015
[6] www.eprocure.gov.in, last visited 20th July 2017
[7] Cryptography and Network Security: Principles and Practice by William Stallings
[8] Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier, Tadayoshi Kohno
[9] https://tendersodisha.gov.in/nicgep/app**,** last visited 20th July 2017
[10] http://nicca.nic.in, last visited 20th July 2017
[11] A method for obtaining digital signature and public key cryptosystems by R.L Rivest, A.Shamir and L. Adleman
[12] Information Security Theory and Practice, Dhiren R. Patel, 2008 Edition
[13] Cryptography and Network Security, Atul Kahate, Second Edition
[14] Cryptography and Information security, V.K. Pachghare, 2009 Edition
[15] Security in Computing Charles P.Pfleeger , Shari Lawrence Pfleeger, Third Edition
[16] Principles and Practices of Information Security, 2009
[17] Mark Stamp's Information Security, Principles and Practice, Deven N.Shah
[18] Computer Security Art and Science, Matt Bishop, 2003
[19] Information Security Policies, Processes and Practice, 2008
[20] "e-Governance", available at http:// india.gov.in, last visited 20th July 2017

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Shaikh Imtiyaj. "Digital Signature Certificate: A Great scientific Knowledge for Nation Development ." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 56-60.