ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 1 , January 2015

# Digital Signature Certificate: A blessing for e-Governance Application in Human Development

Shaikh Imtiyaj, N.R Biswal, T.P Ray, Dr A.K Hota

C.V Raman College of Engineering,BPUT, Bhubaneswar,Odisha,India
Scientist, Ministry of Electr & IT, Bhubaneswar,Odisha,India
Scientist, Ministry of Electr & IT, Bhubaneswar,Odisha,India
Scientist, Ministry of Electr & IT, Bhubaneswar,Odisha,India

**ABSTRACT**: Information and Communication Technology is being increasingly used in daily life of a common man and it has become the nucleus 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. Now a days, departments, business sectors and customers alike collect, store and transmit vast amount of information electronically and they want to believe that this 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) 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. A DSC provides high level of security for online transactions.This study focuses on DSC, implementation of Message Digest algorithm and different opportunities of e-Governance application and provides a model for better implementation of e-Governance application in the country. The usage of DSC in applications such as 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; OJEE Counseling, Collectorate Offices, Registration Offices and many more areas is gradually increasing day by day, improving success in carrying out business functions. 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

## I. INTRODUCTION

As Homo sapiens advanced from the food gathering jungle man of ancient era to e-governed urban man of 21$^{st}$ century, greater emphasis has been laid on utmost utilization of the intellect linking it to technology based human development. 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 has become the nucleus part of providing the better governance 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.

### *A.* 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

### *B.* e-GOVERNANCE DEVELOPMENT MODELS

The e-Governance Models are

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

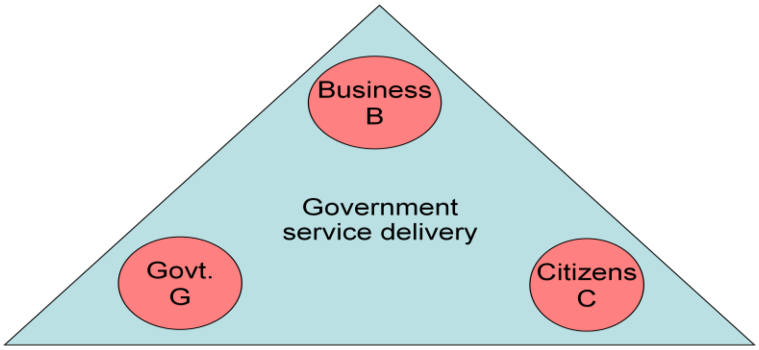


Figure.1- Governance Development Model

## II. LITERATURE SURVEY

DSC is based on MD5 algorithm from Cryptography. In the recent years much progress has been made in the design of practical one-way hashing algorithms which is efficient for implementation by both hardware and software. Noteworthy work includes the MD family which consist of three algorithms MD2, MD4, MD5 and also Secure Hash Algorithm-SHA-1 which produces message digest of 160bits long was the best established of existing SHA hash functions and employed in several widely used security application and protocols. MD5 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.

### *A*. Cryptography

Cryptography means information hiding from unauthenticated persons or programs. It is the application of modern techniques by which modern text (Plain text) is modified in to unintelligible text (cipher text). This technique is otherwise called Encryption. In past cryptography was being done by a common key (Symmetric Key Cryptography) but due to technological advancement now a days we use different key for the encryption process (Asymmetric Key Cryptography). 1. Symmetric Key Cryptography 2. Asymmetric Key Cryptography

1. Symmetric Key Cryptography : In symmetric key cryptography the sender sends the message by encrypting the message by a key say 1 k . The receiver after receiving the cipher text decrypts the message by using the same key 1 k . It's assumed here that both the parties use a common key and the transmission of cipher text is done in an insecure channel. This system is flawed if the key 1 k is leaked i.e. if it's known by the adversary.

2. Asymmetric Key Cryptography: It's otherwise known as public key cryptosystem or public key encipherment, we have the same situation as of symmetric key cryptosystem, with a few exception. First, there are two keys instead of one, one public key and one private key. To send a secured message, the sender encrypts with receiver's public key. To decrypt the message the receiver uses his own private key.

### *B.* DIGITAL SIGNATURE CERTIFICATE

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. A 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 and eToken

### *C.* 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**.

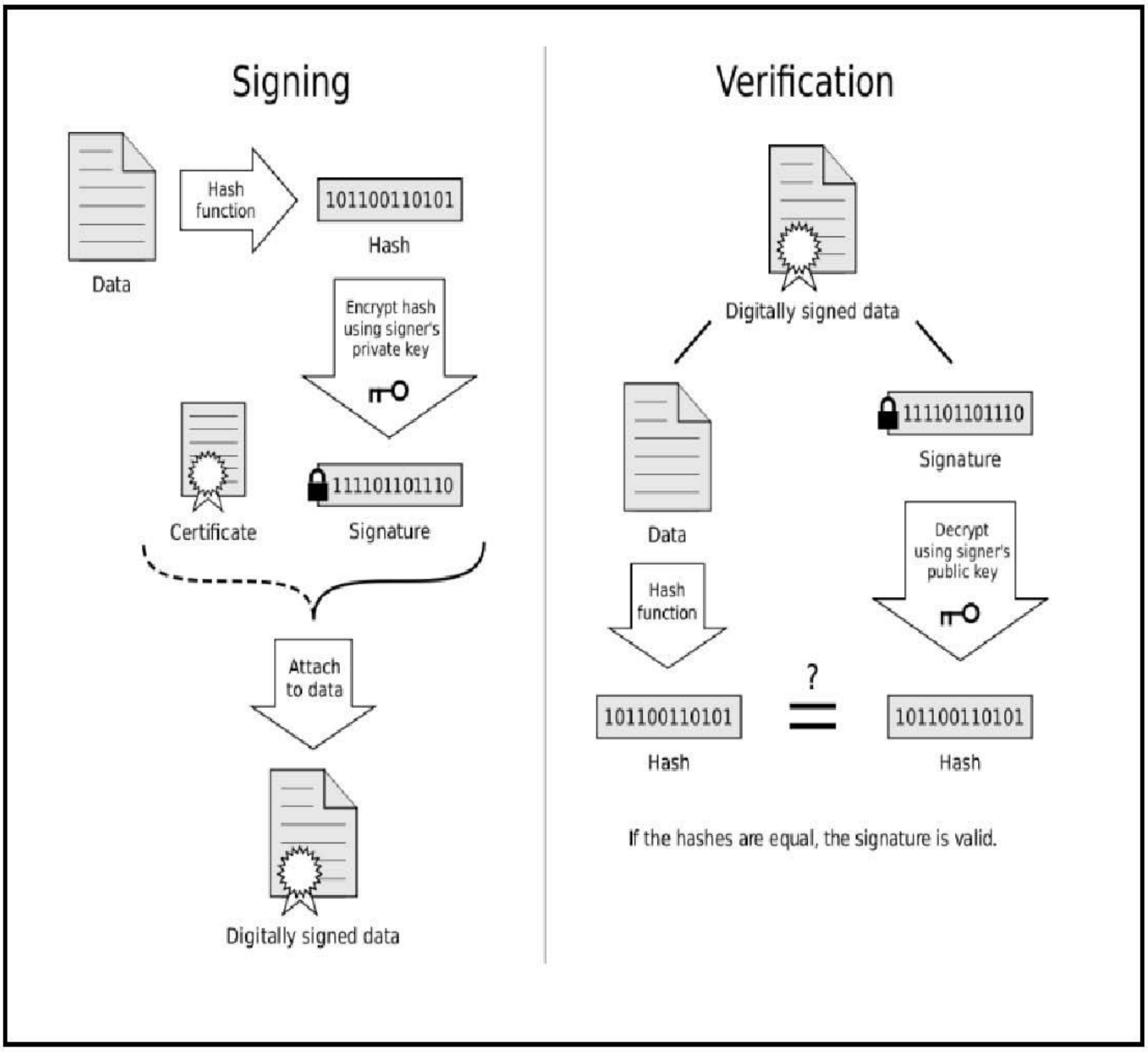


Figure.3- DSC working process

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.

```
importjava.security.*;
class Md5FeeduDemoTest {
public static void main(String[] a) {
try {
MessageDigest md = MessageDigest.getInstance("MD5");
System.out.println("Message Digest5 information: ");
System.out.println("   Algorithm = "+md.getAlgorithm());
System.out.println("   Provider = "+md.getProvider());
System.out.println("   toString = "+md.toString());

        String input = "";
md.update(input.getBytes());
                byte[] output = md.digest();
System.out.println();
System.out.println("MD5(\""+input+"\") =");
System.out.println("   "+bytesToHex(output));

input = "xyz";
md.update(input.getBytes());
                output = md.digest();
System.out.println();
System.out.println("MD5(\""+input+"\") =");
System.out.println("   "+bytesToHex(output));

input = "abcdefghijklmnopqrstuvwxyz";
md.update(input.getBytes());
                output = md.digest();
System.out.println();
System.out.println("MD5(\""+input+"\") =");
System.out.println("   "+bytesToHex(output));

     } catch (Exception e) {
System.out.println("Exception: "+e);
     }
   }
public static String bytesToHex(byte[] b) {
     char hexDigit[] = {'0', '1', '2', '3', '4', '5', '6', '7',
                      '8', '9', 'A', 'B', 'C', 'D', 'E', 'F'};
StringBufferbuf = new StringBuffer();
for (int j=0; j<b.length; j++) {
buf.append(hexDigit[(b[j] >> 4) & 0x0f]);
buf.append(hexDigit[b[j] & 0x0f]);
     }
returnbuf.toString();
```

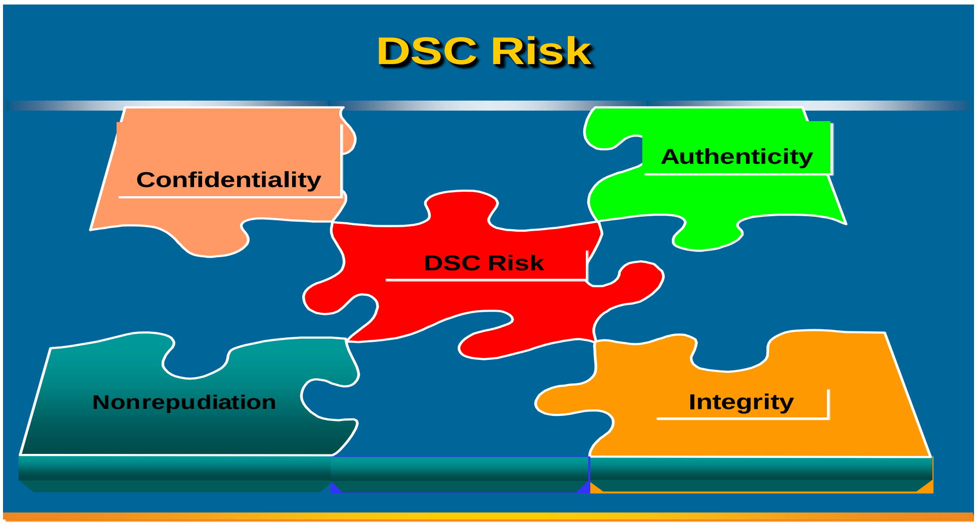
```
   }
}
```

## IV. CLASSES OF DIGITAL SIGNATURE CERTIFICATE

Depending upon requirement of assurance level and usage of DSC, the type of classes are Class-1 Certificate, Class-2 Certificate and Class-3 Certificate. Class-1 Certificate provides minimum level of assurance. 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 Certificateprovides 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.

### *A.* DSC RISK



Shaikh Imtiyaj

Figure.4- DSC Risk

## IV. IMPLEMENTATION

Sending and receiving digitally signed and encrypted emails

For signing web forms

e-tendering documents

e-Procurement

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;

OJEE Counseling

Collectorate Offices (eDistrict)

Registration Offices
Establish SSL encrypted secured sessions between website and the user in web based transaction

## V. CONCLUSION

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. 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]LeinHarn, Jian Ren, Changlu Lin, 'Design of DL-based certificate less digital signatures', The Journal of Systems and Software 82 pp.789–793 , 2009
[2] B. A. Fourazan, DebdeepMukhopadhyay,'Cryptography and Network Security', Tata McGraw Hill, 2nd edition,pp.15,210-234,2010
[3] Lee, Chang, 'Strong designated verifier signature scheme', Computer Standard and Interface, 31, 2009
[4] Al-Riyami, S., Paterson, K., 'Certificateless public key cryptography'.Advances in Cryptology – AsiaCrypt, LNCS, vol. 2894. Springer-Verlag, pp. 452–473,2003
[5] Bellare, M., Namprempre, C., Neven, G.,. 'Security proofs for identity-based identification and signature schemes'. Advances in Cryptology – EuroCrypt'04, LNCS, vol. 3027. Springer-Verlag, pp. 268–286, 2004
[6] Cha, J., Cheon, J.H., 'An identity-based signature from gap Diffie-Hellman Groups'. Public Key Cryptography – PKC'03, LNCS, vol. 2567.Springer-Verlag, pp.18–30. 2003
[7] Chen, X., Zhang, F., Kim, K.,. A new ID-based group signature scheme from Bilinear pairings. WISA'03, LNCS, vol. 2908. Springer-Verlag, pp. 585–592,2003
[8] W.Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on information theory, vol.22,1976.
[9] Alfred M., Oorschot P., and Vanstone S., Handbook of Applied Cryptography, CRC press, 1997.
[10] Stallings W., Cryptography and Network Security Principles and Practices, Prentice Hall Press Upper Saddle River, 2010.
[11] Goldwasser S., Micali S., and Rivest R., "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," Journal on Computing, vol. 17, no. 2, pp. 281-308, 1988.
[12] Ilya M., "Hash Functions: Theory, Attacks, and Applications," in Proceedings of Microsoft Research, Silicon Valley Campus, pp. 1-22, 2005.
[13] Rivest R., Shamir A., and Adleman L., "A Method for Obtaining Digital Signature and Public-Key Cryptosystems," Communication of The ACM, vol. 21, no. 2, pp. 120-126, 1978.
[15] William S., Cryptography and Network Security, Principles and Practice, Prentice Hall of India, 2005.
[16] "Digital Signature," available at: http:// http://nicca.nic.in , last visited 20th Jan 2015
[17] "e-Governance," available at http:// india.gov.in , last visited 20th Jan 2015