Unit 2: Digital Signature Certificate

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Digital Signature Certificate
- Types and Classes of Digital Signature Certificates
- Certifying Authorities issuing digital signatures
- Advantages and disadvantages of Digital Signature Certificates
- Statutory provisions related to Digital Signature Certificates

1.2 INTRODUCTION

A Digital Signature Certificate is a digital key used to validate and certify the identity of an individual digitally. Such a digital Signature Certificate is issued by a certifying authority. Digital Signature Certificates are created by use of public-key encryptions and form the digital equivalent of physical certificates in electronic format. Digital Signature Certificates form a useful way of signing documents electronically. Similar to physical documents being signed manually, Digital Signature Certificates serve the purpose of digitally signing electronic documents. As per the provisions of the Information Technology Act, 2000, Digital Signature Certificates are considered to be admissible in a court of law.[81] Such Digital Signature Certificates can stay valid for up to a minimum of one year to a maximum of three years. Digital Signature Certificates can be used by both individuals and/or organizations. Digital Signature Certificates function based on MD5 algorithm associated with cryptography, which is, in essence, a 'Message-Digest Algorithm', that receives a message of any length as input and releases as output a 128-bit result which is a 'message digest' based on the input.[82]

Today, India is one of the few nations that have laws associated with Digital Signature Certificates. As per the existing laws, all authorized signatories of organizations and any other professional having the authority to *inter alia* sign documents shall be required to obtain the Digital Signature Certificates. Such group of persons could include but not be limited to directors of companies, auditors or chartered accountants, practising company secretaries or those engaged in jobs, officials working at banks etc. Once the Digital Signature Certificate has been issued and received by the applicant, the certificate can be used by the holder to sign any document online.

1.3 TYPES AND CLASSES OF DIGITAL SIGNATURE CERTIFICATES

There can be four kinds of Digital Signature Certificates, which are as follows:

(a) ***Sign*** – Sign Digital Signature Certificates can be solely used for signing documents. While on one hand, its usage signifies integrity of the data as well as the signer, on the

[81] FeghhiJ and P Williams, Digital Certificates: Applied Internet Security 1st ed Reading, MA: Addison-Wesley [1999]
[82] StallingsW, Cryptography and Network Security, 3rd ed. EnglewoodCliffs, NJ: Prentice-Hall, 2002

other, it ensures that the data does not get altered or tampered. Commonly, Digital Signature Certificates are used with respect to the filing of tax returns.[83]

(b) ***Encrypt*** – Encrypt Digital Signature Certificates can solely be used to encrypt a document, as popularly used by companies to encrypt and upload documents and/or send across classified information. Encrypt Digital Signature Certificates are used in association with e-commerce documents and other documents, legal or otherwise, that are extremely confidential in nature and need extensive protection.

(c) ***Sign and Encrypt*** – Sign and Encrypt Digital Signature Certificates can be used to together serve the individual purposes of each of sign and encrypt Digital Signature Certificates. It helps authenticate information as well as maintain their confidentiality at the same time.

(d) ***Server Certificate*** – These kinds of certificates are used in identifying a server by means of the hoist name and/or IP address that they contain, and are used for ensuring secure communication of data using the internet.

Primarily, there could be three classes of Digital Signature Certificates. They are as follows:

(a) Class 1 Certificate – These Digital Signature Certificates are issued to individuals and/or private users to authenticate the details of the user such as name, email address etc.

(b) Class 2 Certificate – These Digital Signature Certificates can be issued to individuals as well as organizations for both personal as well as professional use. The purpose of its use is to reaffirm and authenticate the details of the signer. It is used most commonly n instances of electronic form filling, income tax filing, registration is done online, email attestation, application for GST etc.

(c) Class 3 Certificate – These Digital Signature Certificates are high assurance certificates that more secure in comparison to Class 2 Certificates, and are arguably considered to be the safest. They provide high safety and security with respect to information and are used mainly in e-commerce and online trading involving privileged information and big amounts of money. Class 3 Digital Signature Certificates are only issued once the holder makes a physical appearance before the certifying authority.[84]

[83] Denning, D E Cryptography and Data Security. Reading, MA: Addison-Wesley(1982)
[84] Stallings, W Cryptography and Network Security: Principles and Practice, 4th ed Englewood Cliffs, NJ: Prentice Hall(2006)

*

Class 1	Class 2	Class 3
Certificates are issued to government organizations, business organizations as well as individuals.	**Certificates may be issued to those individuals who belong to business and/or government organizations that are willing to verify the information submitted by such individual subscriber. Certificates can also be issued to organizations that are well-known and are capable of self-verifying the information submitted.[85]**	**Certificates can be issued to both individuals as well as organizations.**
Used to enhance the security associated with personal emails and personal web browsing, and is used primarily to that effect.	**Used for aiding in an organization's administrative and functional needs.**	**Used extensively for e-commerce applications, electronic banking, other online services that rely on online memberships and subscription, etc.**
Assurance provided is of the lowest level in comparison to other kinds of certificates.	**Assurance provided is of more than Class 1 certificates. However, the verification process**	**The validation procedure involved provides assurances stronger than that provided by Class 1**

[85] Practical Security Aspects of Digital Signature Systems: Florian Nentwich, Engin Kirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna(JUNE2006)

	involved with the issuance is more rigorous than that involved in association with Class 3 certificates.	**and Class 2 certificates.**
Certificates help in confirming a user's name and email address.	**A digital certificate signed by the Certifying authority is given to the head of an organization or his/her nominee so that the process of issuing further Certificates can be initiated.**	**Significant assurances associated with the identity of subscribers are provided following the personal physical appearance of such subscribers before the certifying authority.**

While the certifying authority has the right to issue more classes of certificates, it has to be nevertheless ensured that the same be expressly defined along with their purpose as and when issued.[86]

In order for a Class 3 Certificate to be issued, certain requirements that need being fulfilled are as follows:

Individual Applicant	**Company Applicant**	**Government Applicant**
After the application is filled and submitted, the individual applicant will need to be present physically before the Registration Authority with an original copy of one of the following	**An individual representing the company that has subscribed for the certificate has to be present physically before the Registration Authority with proof of ownership and other details**	**An individual representing a government applicant that has subscribed for the certificate has to be present physically before the Registration Authority with a letter on the official letter of the subscriber**

[86] Banday, M Tariq & Dethe, C (2011) Easing PAIN with Digital Signatures. International Journal of Computer Applications

documents : **i) Passport** **ii) Voter ID Card** **iii) PAN Card** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**associated with the subscriber company.** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**which must contain the following:** i) **Name of the organization** ii) **Administrative department** iii) **Address of the subscriber** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**

1.4 CERTIFYING AUTHORITY

A ***'Certifying Authority'*** is an entity who has been granted the authority of issuing Digital Signature Certificates as per the provisions of section 24 of the Information Technology Act, 2000. All the licensed Certifying Authorities and their contact numbers are available in the public domain.

A Certifying Authority can directly be approached by an applicant with supporting documents of original and self-attested copies for acquiring a Digital Signature Certificate. A Certifying Authority could also be approached for a Digital Signature Certificate also with only the eKYC based authentication details associated with Aadhar Card in which case no supporting documents shall be required. A letter containing the necessary information issued and certified by the bank wherein the applicant of the Digital Signature Certificate holds an account is also considered valid and sufficient for acquiring a Digital Signature Certificate.[87]

[87] Afrianto, Irawan & Heryandi, Andri & Finandhita, Alif & Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

The applicant of a Digital Signature Certificate holds a private key that corresponds to the public key that is to be listed in the certificate, and further holds a private key which creates the digital signature. The public key which is listed in the Digital Signature Certificate is used to verify the digital signature that the applicant affixes using the secure private key. Once applied, the Certifying Authority could take around three to seven working days for issuing a Digital Signature Certificate.

1.5 UTILITY OF DIGITAL SIGNATURE CERTIFICATES

The utility of Digital Signature Certificates lies in the fact that Digital Signature Certificates can be used as a means of electronic proof of identity of an individual. Digital Signature Certificates can be further used for signing documents digitally or accessing information or availing services over the internet.[88]

Digital Signature Certificates further provide benefits of privacy to their holders and also help authenticate and authorize entities to get involved *inter alia* in electronic transactions. While on one hand Digital Signature Certificates and their usage have been given legal validity owing to the provisions of the Information Technology Act, 2000, on the other, they can also provide a high level of security for online transactions by encrypting information only for the purposes of intended use by the intended recipient(s). The added advantage with respect to Digital Signature Certificates ensures that the information involved remain unaltered in spite of transition.[89]

The major advantages associated with the use and implementation of a Digital Signature Certificate are as follows:

(i) Prevention of Fraud – Use of Digital Signature Certificate eliminates the possibility of fraud by entirely eliminating the scope of alteration therein or creating a duplicate thereof.

(ii) Preserving integrity – Use of Digital Signature Certificates established the validity of a document in all legal, formal and official aspects.

[88] Zheng Y, Imai H and Imai, H (Ed) 2007 Public Key Cryptography, Springer, ISBN: 9783540656449

[89] FIPS (1996) Digital Signature Standard (DSS), FIPS PUB 186-3, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-890, available online at: <http://csrc.nist.gov/publications/fips/fips186-3/fips_186- 3.pdf>

(iii)Advantages in Online Banking – Businesses depending on online banking procedures are extensively benefitted by the use of Digital Signature Certificates.

1.6 INGREDIENTS OF A DIGITAL SIGNATURE CERTIFICATE

The ingredients of a Digital Signature Certificate *inter alia* include the following details:

(a) The name of the individual owing the digital signature certificate
(b) The public key held by the owner of the digital signature certificate
(c) The date of expiry associated with the public key held by the owner
(d) The name of the certifying authority issuing the digital signature certificate
(e) The serial number associated with the digital signature certificate
(f) The digital signature of the owner/user of the digital signature certificate

1.7 SUBSCRIBER'S OBLIGATIONS

Besides imposing statutory obligations on the Certifying Authorities issuing Digital Signatures Certificates, the provisions of the Information Technology Act, 2000 also impose certain obligations on the subscribers applying for the Digital Signature Certificates. Such obligations are as follows:

i) Providing correct information devoid of errors, omissions, misrepresentations etc. in the application for the Digital Signature Certificate.
ii) Accepting the Digital Signature Certificate as generated by the Certifying Authority if all the information contained in the Digital Signature Certificate applied are validated to be true.
iii) In the event there are any changes required to be made in the Digital Signature Certificate of the subscriber to prevent the certificate from being misleading, the same shall be correctly provided by the subscriber forthwith after such change takes place.
iv) Ensuring the protection of the private key in a secure medium.

v) Ensuring that the certificate is terminated in case the information contained in such certificate is inaccurate and misleading.

The Act lists down the duties of subscribers in sections 40, 40A, 41 and 42 in the following manner.[90]

Section 40 *– Generating Key Pair – Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.*

Section 40A *– Duties of subscriber of Electronic Signature Certificate – In respect of Electronic Signature Certificate, the subscriber shall perform such duties as may be prescribed.*

Section 41 *– Acceptance of Digital Signature Certificate – (1) The subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate –*

(a) to one or more persons;

(b) in a repository;

or otherwise demonstrates his approval of the Digital Signature Certificate in any manner;

(2) By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

[90] Ross Anderson and Eli Biham (1996). Tiger: A Fast New Hash Function, Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, pp. 89—97

1.8 DISADVANTAGES OF DIGITAL SIGNATURE CERTIFICATES

In spite of the extensive advantages associated with Digital Signature Certificates, there are a handful of disadvantages that arise from the issuance, use and implementation of Digital Signature Certificates, such as follows:

(a) Financial disadvantage: Certifying Authorities that issue Digital Signature Certificates require a monthly subscription from the applicant of such certificate. Such monthly subscription and the hefty costs involved therewith could become a liability on the entity or individual applying for the Digital Signature Certificate.[91]

(b) Equipment Cost: Electronic signatures that are required to be read by upgraded technology which warrants the extensive investment. Such expenses might become too heavy for certain applicants of Digital Signature Certificate.

(c) Deterrence on Clients: Application for and implementation of Digital Signature Certificates involve the use of certain applications and advanced forms of technology. Since the system of issuance and use of Digital Signature Certificate involve an extensive understanding of sophisticated technology and functioning of equipment, some clients might face trouble using Digital Signature Certificate, which could in turn cause deterrence towards using Digital Signature Certificates.[92]

1.9 LET'S SUM UP

In this chapter, we have studied the concept of digital signature certificate along with the types and classes. Furthermore, we also studied about how certifying authority issues the certificate and the obligations of the subscriber. Finally, we have ended our discussion with the advantages

[91] CCA. (2009). Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, CCA India, version 2.4 updated on 14th June 2011
<http://cca.gov.in/rw/resource/dsc _guidelines_r2_4.pdf>

[92] IT ACT (2000), The Information Technology Act, 2000, Government of India
<http://www.mit.gov.in/sites/ upload_files/dit/files/downloads/itact2000/itbill2000.pdf>

and disadvantages of digital signature certificate along with the statutory provisions pertaining to it.

1.10 FURTHER READING

- http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf
- Roy, Dr. Abhishek & Karforma, Sunil. (2012). A survey on digital signatures and its applications. JCIT. 3. 45-69.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a Digital Signature Certificate?

A. A Digital Signature Certificate is the electronic equivalent of physical form of certificates that can act as proof of identity for individuals, or sign documents digitally.

2. Who issues Digital Signature Certificates?

A. An individual or an entity authorised to grant Digital Signature Certificates as per section 24 of the Information Technology Act, 2000.

3. What are the classes of Digital Signature Certificates?

A. Digital Signature Certificates can be classified into three classes – Class 1, Class 2 and Class 3. Class 1 certificates are issued to users to authenticate their details such as name, email address etc. Class 2 certificates verify the identity of a person against a trusted, pre-verified database. Class 3 certificates involve the appearance of the applicant before the certifying authority for proving the identity.

4. How long do Digital Signature Certificates remain valid?

A. Digital Signature Certificates can stay valid for a minimum of one year to a maximum of three years.

5. What is the legal status associated with Digital Signature Certificates?

A. Digital Signature Certificates are admissible in courts of law in accordance with the provisions of the Information Technology Act, 2000.

1.12 ACTIVITY

Describe the issues and challenges associated with addressing identity theft in cyberspace in light of digital signature certificates and their applicability. (800 words)