

BUSINESS LAWS
II B.COM (CA& G) IV Sem
DIGITAL SIGNATURE

BY
B.KRISHNAVENI
LECTURER IN COMMERCE
GOVERNMENT DEGREE COLLEGE (W)
HINDUPUR
ANANTAPUR DISTRICT

WELCOME



Contents

1 Introduction

2 Meaning and Definition of Digital Signature – IT
Act, 2000

3 Digital Signature Vs Electronic Signature

4 Digital Certificates

5 Significance of Digital Signature

6 Limitations of Digital Signature

7 Legal Implications

8 References

Learning objectives

Objective of this presentation is enabling the student in understanding the following:

Meaning of Digital Signature

Digital Signature in Information Technology Act,
India

Significance of Digital Signature

Limitations of Digital Signature

Legal Implications

Introduction

- Conventional signatures are the marks made by persons to authenticate a document, and assure the receiver that he has signed it personally.
- Wide spread use of internet has resulted in cyber crimes which mandated for stringent legislation for protecting the users from the crimes associated with internet.
- At this juncture Digital signature is one of the various measures introduced by IT Act, 2000 to curb the fraudulent use of technology.
- Hence, the concept of digital signature has come up. The online transaction requires unique and strong protection which is served by electronic signature.
- Hand written signature is prone to forgery and tampering and this limitation can be overcome by digital signature to a greater extent.



Meaning of Digital Signature – Information Technology Act, 2000

Digital signature is a mathematical scheme to verify the authenticity of digital documents or messages.

Digital Signature under Information Technology Act, 2000 – primary law in India dealing with cyber crime and e-commerce.

According to the Information Technology Act, 2000, digital signatures mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Further, the IT Act, 2000 deals with digital signatures under sections 2, 3 and 15.

According to Sec 2(1) (p) digital signature means ‘authentication of any electronic record using an electronic method or procedure in accordance with the provisions of section 3.

The provisions of Sec 3 of the Information Technology act, 2000

- Any subscriber can affix his digital signature and hence authenticate an electronic record.
- An asymmetric crypto system and hash function envelop and transform the initial electronic record into another record which affects the authentication of the record.
- Also, any person in possession of the public key can verify the electronic record.
- Further, every subscriber has a private key and a public key which are unique to him and constitute a functioning key pair.

Sec 15 of the Information Technology Act – secure digital signature

a digital signature is considered secure if, by application of a security procedure agreed to, by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which related in such a manner that if the electronic record was altered the digital signature would be invalidated.

A digital signature establishes identity of sender while filing the documents through internet.

Digital Signature Vs Electronic Signature

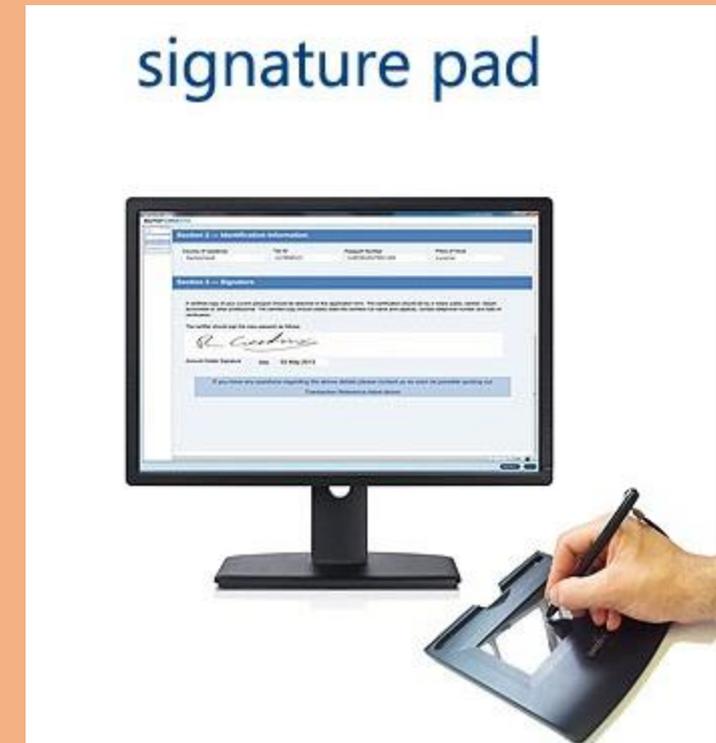
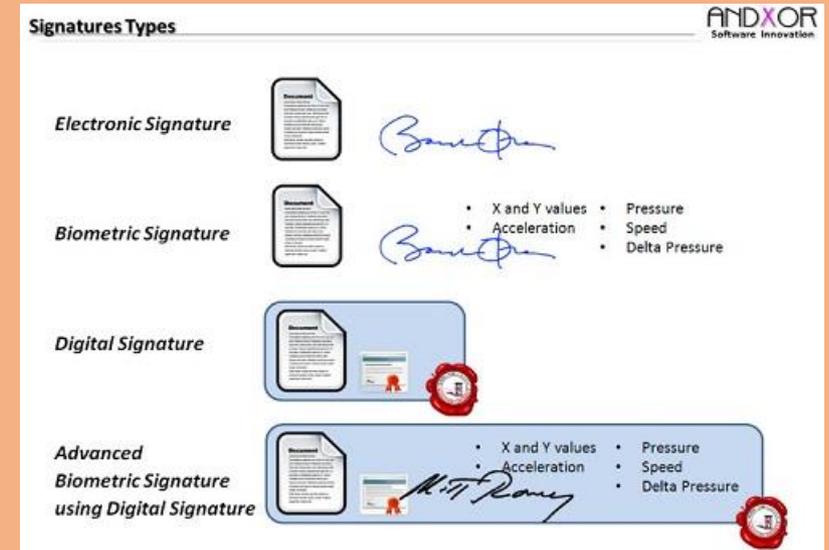
The Information Technology act, 2006 replaces the word 'digital' with 'electronic' at several places in the principal Act slightly differentiating the two. Electronic signature is comprehensive and digital is one of the electronic forms.

The main difference between the two is that digital signature is mainly used to secure documents and is authorized by certification authorities while electronic signature is often associated with a contract where the signer has got the intention to do so.

Digital signature is an electronic signature but all electronic signatures are not digital signatures.

Electronic signature- all the methods available for authentication while dealing with online documents; password, PIN, Biometric Signature, digital signature.

Digital signature is an asymmetric cryptosystem which has a key pair – Public key and Private key
Public key verifies and the private key authenticates the online document.
Key here means a unique number.

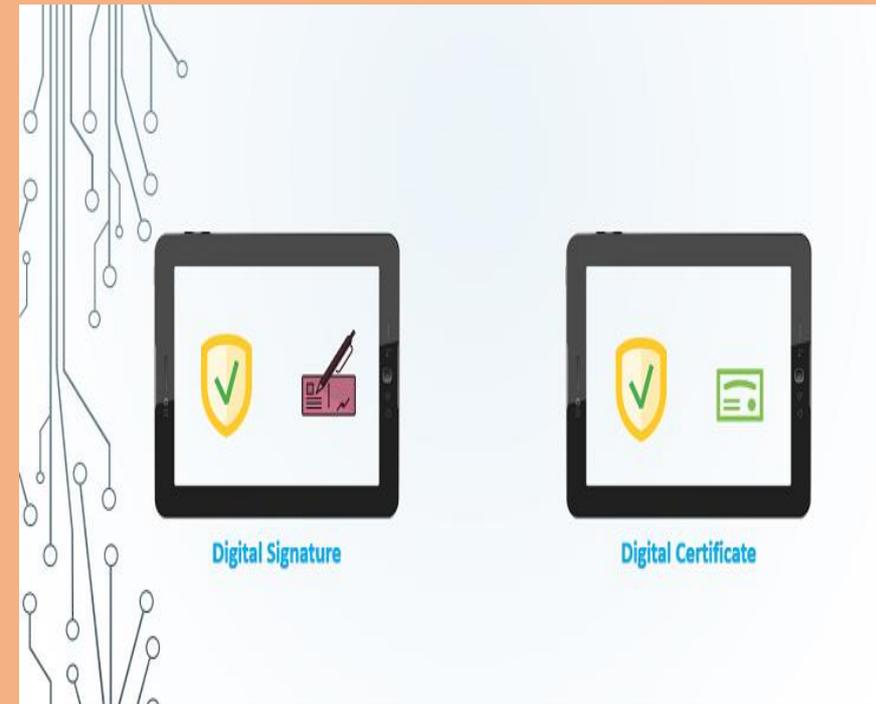


Digital Certificates

A digital certificate is used to validate the document to ascertain its authenticity if it has not been forged. This plays a pivotal role in verifying the identity of the original person with the signature.

Digital Signature is often authorized

by certification authorities that are responsible for providing digital certificates that can be compared to licenses or passports.



Significance of Digital signature

The following features of digital signatures reflect their significance in online transactions:

- Authenticity
- Integrity
- Non repudiation

In addition to the above digital signatures reduce time and cost in sending the documents by courier or by a person.

Tampering and forgery can be avoided

Digitally signed documents can be tracked easily

Digitally signed are equally valid as pen on paper signature in court of law

Limitations of Digital Signature

Limitations of digital signature are because of laws regarding cyber security which may become a challenge when in case of legal issues both parties have to purchase the certificates for digital signature in order to use it.

It requires efforts to identify and review new malware signatures.

Inability to detect zero day attacks

However, to conclude it can be emphasised that advantages of digital signature outweigh the disadvantages and has proved its compelling need for present day business and government.

Legal Implications

The offences related to electronic signature are generally related identity theft, publication of false electronic signature certificate, publication of electronic certificate with fraudulent purpose. Indian IT Act punishes under sections 66C, 71, 73 and 74 based on the offence with fine, imprisonment or both as the case may be.

References

- [www.legalserviceindia.com>article>1212-Digital Signatures](http://www.legalserviceindia.com/article/1212-Digital_Signatures)
- <http://www.differencebetween.net/technology/difference-between-digital-signature-and-electronic-signature/#ixzz6JkhGQGcG>
- digitalindiainsight.com
- link.springer.com; ‘Intrinsic Limitations of Digital Signatures’
- indiacode.nic.in
- meity.gov.in

THANK YOU