

INFORMATION TECHNOLOGY, 2000

Section - II

Sachin Hiraskar : 8310357954 (Telegram)

This chapter includes : A) public key

• Introduction

• Definition

• Physical signature & E-signature

• E-communication

• Definition of E-signature

• Section E - signed & E-signature

• E-signature certificate

• Physical

• Misconception

1. INTRODUCTION

of India to India. India is also home to various traditional technologies

of non-appropriability

• Negative statement (other than change)

• Power of attorney

• Impairment for sale or conveyance of imm. prop.

2. DEFINITIONS

1. Cyber Security :

Means protection of info, equipment, devices, computer, computer network, communication device for large sized base in their unauthorised access, use, disclosure, destruction, modification or distribution.

ii. Digital signature :

Means authentication of any E-record by a subscriber by means of an E-record in accordance with sec. 3 provision

iii. Electronic Stamp :

With signature in information, means any info generated, sent, received or stored in media, magnetic, optical, computer, memory, micro film, computer generated micro film or similar device.

iv. Electronic signature :

Means authentication of any E-record by a subscriber by means of E-technical specified in standard specified in include digital signature.

v. Private Key :

Means the key of a key pair, used to create a digital signature.

vi. Public Key :

Means the key of a key pair, used to verify a digital signature certificate.

vii. Key pair :

It is an asymmetric crypto system, means a pair key & it's mathematically related public key, which are so related that public key can verify a digital signature created by private key.

viii. Intermediary :

Means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes, telecom service providers, network & internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online insurance players & cyber cafe.

3. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

a) It is a signature or a valid method of authentication.

b) Authentication is made by use of "asymmetric crypto system & hash function, which involves identification of E-record from creation electronic record.

c) Asymmetric crypto system is a system of key pair consisting private key to create EC public key to verify EC.

d) Verification of E-record is done by use of public key of the subscriber.

e) The private key & the public key are unique in the subscriber & constitute a functioning "key pair".

1. Hash function is for security purpose which creates unique number

a) Authentication must be done by technique which is suitable

b) Authentication can be considered as message if authentication is made by subscriber by using private key

c) Such signing must under the control of signing user

d) Any alteration in EC after signing is detectable

e) Any alteration in large after it's authentication by EC is detectable

f) ECs have been arrived legal recognition in India.

2. E-VERIFICATION

i. Sec 4 :

Legal recognition of E-record, if done in following manner

• Type within time

• Printed form

• Any procedure or otherwise which is sufficient for authentication

ii. Sec 5 :

Legal recognition for EC, if any info provided that info shall be substantiated by signing the signature in any other way, signature of any person :

• It can be done also by means of EC and it is valid for understanding anything contained in such info

iii. Sec 6 :

Legal recognition in E-signing with given agency in given way

• Thing any form, app or other doc

• Grant of any document

• Receipt or payment of money made in signed E-record

iv. Sec 10A :

Contract are also enforceable, if following are made electronically

• Communication of proposal

• Acceptance of proposal

• Revocation of proposal

v. Attribution and dispatch of E-records

a) Record is said to be substituted by signature when

• Sent by original sender

• Sent by any person authorized by original sender

• Sent by person whose system, host, device, automatically on behalf of originator.

b) Info shall be deemed to be authenticated when

• Type within time

• Any communication by authentic printed form

d) Time of dispatch :

• At per destination the originator is authorized

• Time at which record enters computer system, outside control of originator → If there is no agreement

e) Time of receipt :

• When E-record enters computer system of addressee

f) Security E-records :

• The signature shall be deemed to be a letter, if under the exclusive control of signing only

• The signature creation data used should be signed in such relative password manner

g) Contributing Probability :

• It is a body which carries legal responsibility of to issue, receive, store & provide distribution of E-records

• It means person who has granted a license to issue EC

• Procedure for obtaining EC

• Any person may make app to CA (authorizing authority) in a prescribed manner along with fee

• App shall be accompanied by declaration of person a statement (relating their position)

• CA may grant EC after making necessary inquiry & may issue after giving RBI

h) Compensation of Failure to protect them

When any body (operator, provider, dealing or dealing any person) fails to protect the same due to negligence & is found liable, shall be liable to compensate aggrieved person

5. PENALTY

Sec 43 : Damage to Computer, Computer system, etc.

• Accidental or unintentional damage to computer system, network, or any info

• Damaged or altered any information

• Intentional damage to computer system, network, or any info

• Intentional damage to alter any personal info

• And all affected aggrieved → to pay damages by way of compensation to person so aggrieved

Sec 55 : Tampering with computer source info.

Whoever intentionally destroys or alters any info that is "not" to maintain under any law → tampering upto 3 years or fine upto 2 lakh or both

Sec 56 : Computer related offence.

Whoever intentionally or recklessness with 3 years or fine of upto 2 lakh or both

Implementation upto 3 years or fine of upto 2 lakh or both

Sec 57 : Compensation of Failure to protect them

When any body (operator, provider, dealing or dealing any person) fails to protect the same due to negligence & is found liable, shall be liable to compensate aggrieved person

When such EC shall be liable to compensate aggrieved person

Sachin Hiraskar : 8310357954 (Telegram)