

The Information Technology Act 2000 (Act 21 of 2000)

Published by Ministry of Law, Justice and Company Affairs

- An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as —electronic commercial, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend Bharatiya Nyaya Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- General Assembly of the United Nations by resolution on 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;
- All States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;
- it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

- ❖ Enacted: - 09th June 2000
- ❖ Came into the force: - 17th OCT 2000

1. It shall extend to the whole of India and save as otherwise provided in this act, it applies also to any offence or contravention there under committed outside India by any person.

2. Definitions:-

- ❖ **Addressee** means a person who is intended by the originator to receive the electronic record but does not include any intermediary
- ❖ **Asymmetric Crypto System:** - Means system of a secure key pair consisting of private key for creating digital signature and a public key to verify the digital signature.



8000661414



/basicpay



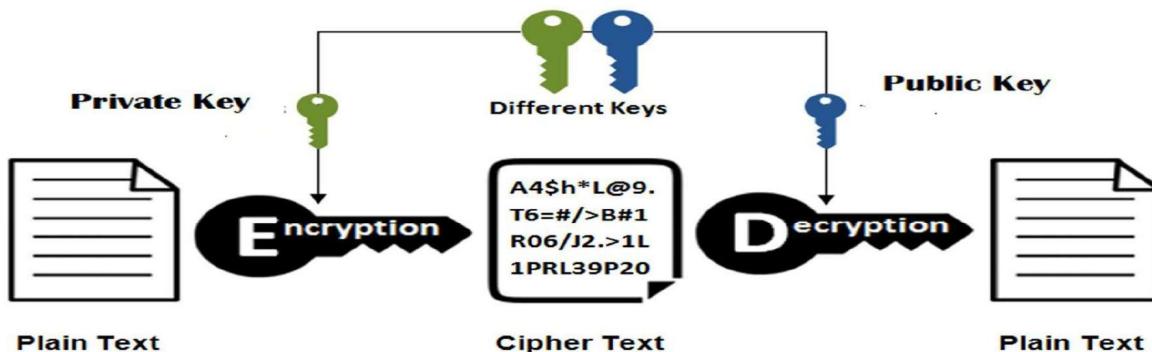
@basicpay



/basicpay

- ❖ **Key Pair:** - Key pair is a asymmetric crypto system means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key
- ❖ **Subscriber:** - Subscriber means a person in whose name the electronic signature certificate is issued.
- ❖ **Hash Function:** - Hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as "*Hash result*" such that an electronic yields the same Hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible.
 - (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
 - (b) that two electronic records can produce the same hash result using the algorithm

Asymmetric Encryption



Public Key & Private Key

- Any person using a *Public Key* of the subscriber can verify the *electronic record*.
- The Private and Public Key are unique to the subscriber and constitute a functioning key pair.



8000661414



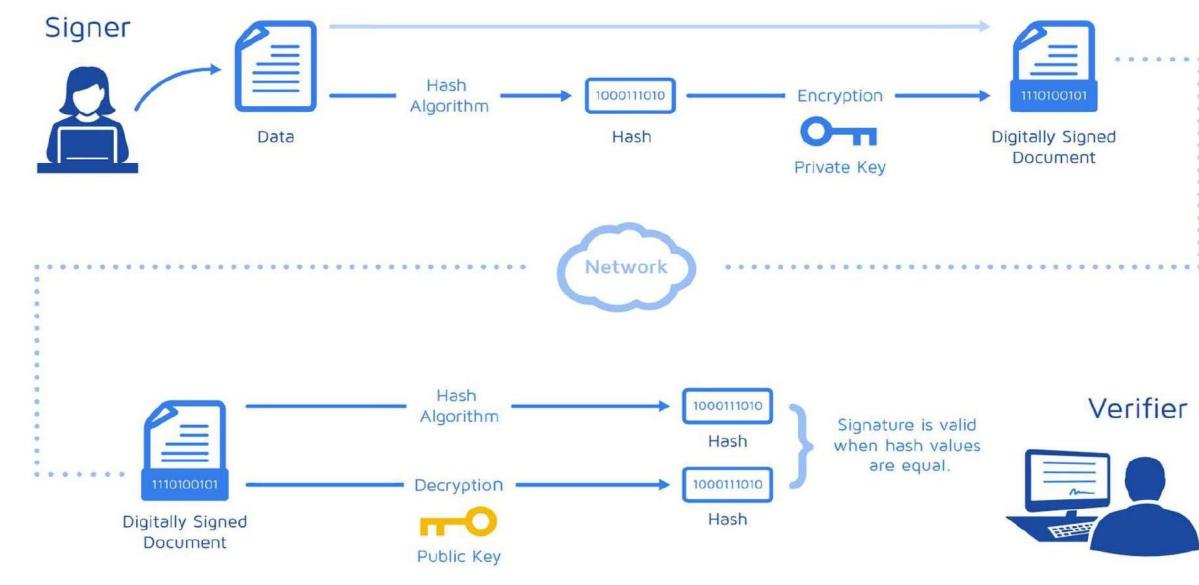
/basicpay



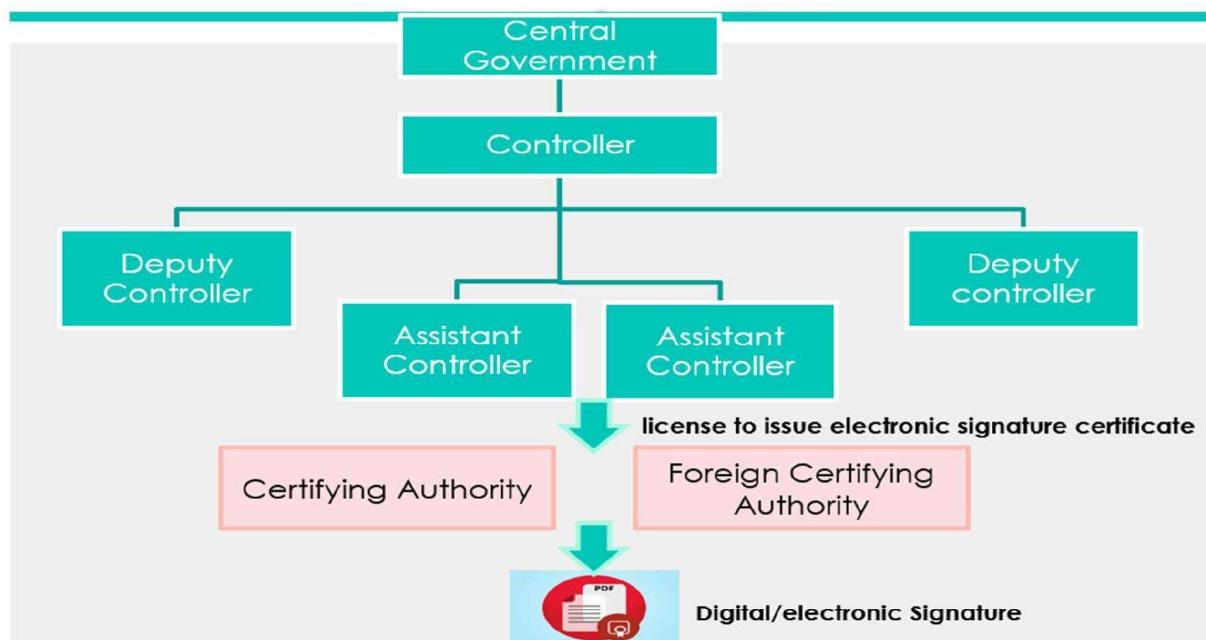
@basicpay



/basicpay



- ❖ **Secure System:** -means computer hardware, software, and procedure that-
 - are reasonably secure from unauthorized access and misuse;
 - provide a reasonable level of reliability and correct operation;
 - are reasonably suited to performing the intended functions; and
 - adhere to generally accepted security procedures;



8000661414



/basicpay



@basicpay



/basicpay

22. Application for license to issue electronic signature certificate: -

- ❖ Payment of such fees, not exceeding Rs.25,000/- as may be prescribed by Govt.

23. Renewal of license: -

- ❖ Not exceeding Rs.5,000/- as may be prescribed by the Central Government and shall be made not less than 45 days before the date of expiry of the period of validity of the license.

25. Suspension of License: -

- ❖ No license shall be suspended for a period exceeding 10 days unless the certifying authority has been given a reasonable opportunity of showing against the proposed suspension

33. Surrender of license: -

- ❖ Every certifying authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the controller.
- ❖ Where any certifying authority fails to surrender a license
 - The person in whose favor a license is issued, shall be liable to penalty which may extend to Rs.5,00,000/- (Five Lakh).

35. Certifying Authority to issue electronic signature certificate: -

- ❖ Every application shall be accompanied by such fee not exceeding Rs.25,000/- as may be prescribed by the central government to be paid the certifying authority.

37. Suspension of Digital Signature Certificate: -

- ❖ A digital signature certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard in the matter.

38. Revocation of Digital Signature Certificate: – A Certifying Authority may revoke a Digital Signature Certificate issued by it–

- where the subscriber or any other person authorised by him makes a request to that effect; or
- upon the death of the subscriber; or



8000661414



/basicpay



@basicpay



/basicpay

- upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

44. Penalty for failure to furnish information, return etc.:-

If any person who is required under this act or any rules or regulations made thereunder to

- (a) Furnish any document, return or report to the controller or the certifying authority fails to furnish the same, he shall be liable to a penalty not exceeding **Rs.15,00,000/- (Fifteen Lakh)**
- (b) Fail to file return or furnish the same (any information, book or other document within the time specified therefor in the regulations he shall be liable to a penalty not exceeding **Rs.50,000/- (Fifty Thousand)** for every day during which such failure continuous.
- (c) Maintain book of account or records: - fails to maintain the same he shall be liable to a penalty not exceeding **Rs.1,00,000/(One Lakh)**- for every day during which the failure continuous.

45. Residuary penalty: -

- Whoever contravenes any rules or regulations made under this act for the contravention of which no penalty has been separately provided shall be liable to pay a compensation not exceeding **Rs.1,00,000/- (One Lakh)** to the person effected by such contravention or a penalty not exceeding
 - **Rs.10,00,000 (Ten Lakh)**, by an intermediary, company or body corporate or
 - **Rs.1,00,000 (One Lakh)**, by any other person.

46. Power to adjudicate (Officer rank of Director in CG/SG Govt): -

- The adjudicating officer/Inquiry officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore.
- Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court

48. Appellate Tribunal: -

- **The Telecom Disputes Settlement and Appellate Tribunal** established under section 14 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), shall, on and from the



8000661414



/basicpay



@basicpay



/basicpay

commencement of Part XIV of Chapter VI of the Finance Act, 2017 (7 of 2017), be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act

57. Appeal to Appellate Tribunal: -

- Every appeal shall be filed within a period of **forty-five days** from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed.
- The appeal filed before the 1[Appellate Tribunal] under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally **within six months** from the date of receipt of the appeal

62. Appeal to High Court: -

- Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within **sixty days** from the date of communication of the decision or order of the Appellate Tribunal to him on any question of fact or law arising out of such order.

65. Tampering with computer source documents: -

- ❖ Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to **three years**, or with fine which may extend **up to two lakh rupees**, or with both.

66. Computer related offence: -

- ❖ If any person, dishonestly or fraudulently, does any act access/ download/ copies/damage/disrupt/destroy/steal/modify/damage a computer without permission of its owner, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to **five lakh rupees or with both.**



8000661414



/basicpay



@basicpay



/basicpay

66A. Omitted

66B. Punishment for dishonestly receiving stolen computer resource or communication device:-

- ❖ shall be punished with imprisonment of either description for a term which may extend to **three years** or with fine which may extend to rupees **one lakh** or with both.

66C. Punishment for identity theft: -

- ❖ Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which **may extend to three years** and shall also be liable to fine which **may extend to rupees one lakh**.

66D. Punishment for cheating by personation by using computer resource: -

- ❖ Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which **may extend to three years** and shall also be liable to fine which **may extend to one lakh rupees**.

66E. Punishment for violation of privacy: -

- ❖ Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which **may extend to three years or with fine not exceeding two lakh rupees**, or with both.

66F. Punishment for cyber terrorism: -

- ❖ Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which **may extend to imprisonment for life**.

67. Punishment for publishing or transmitting obscene material in electronic form:-

- ❖ shall be punished on first conviction with imprisonment of either description for a term which may extend to **three years and with fine** which may **extend to five lakh rupees** and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **five years and also with fine which may extend to ten lakh rupees**.



8000661414



/basicpay



@basicpay



/basicpay

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

- ❖ shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

- ❖ shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

67C. Preservation and retention of information by intermediaries. –

- ❖ Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
- ❖ any intermediary who intentionally or knowingly contravenes the provisions of above section shall be liable to penalty which may extend to Rs.25,000,00 (twenty-five lakh rupees).

68. Power of Controller to give direction –

- ❖ Any person who intentionally or knowingly fails to comply with any order of the controller shall be guilty of an offence and shall be liable to penalty which may extend to twenty-five lakh rupees.

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.

- ❖ The central govt may enhance cyber security and for identification analysis and prevention of intrusion or spread of computer contaminant in the country by notification in official gazette authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.



8000661414



/basicpay



@basicpay



/basicpay

- ❖ Any intermediary who intentionally or knowingly contravenes the above provision shall be punished with an imprisonment for a term which may extend to one year or shall be liable to fine which may extend to one crore rupees or with both

70B. Indian Computer Emergency Response Team to serve as national agency for incident response: -

- ❖ The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.
- ❖ The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security: -
 - collection, analysis and dissemination of information on cyber incidents;
 - forecast and alerts of cyber security incidents;
 - emergency measures for handling cyber security incidents;
 - coordination of cyber incidents response activities;
 - issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
 - such other functions relating to cyber security as may be prescribed.
 - may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.
 - Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction, shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to One Crore rupees or with both.

71. Penalty for misrepresentation. - Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence [electronic signature] Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to five lakh rupees, or with both.



8000661414



/basicpay



@basicpay



/basicpay

72. Penalty for Breach of confidentiality and privacy. - if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable which may extend to **five lakh rupees**.

72A. Punishment for disclosure of information in breach of lawful contract - any person including an intermediary containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be extend to **twenty-five lakh rupees**.

73. Penalty for publishing electronic signature Certificate false in certain particulars. -(1) No person shall publish an [electronic signature] Certificate or otherwise make it available to any other person with the knowledge that-

- (a) the Certifying Authority listed in the certificate has not issued it; or
- (b) the subscriber listed in the certificate has not accepted it; or
- (c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying an [electronic signature] created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

74. Publication for fraudulent purpose - shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

* Amendment vide Gazette Notification SO 4745(E) dated 31.10.2023

[THE FIRST SCHEDULE]

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

Sl. No.	Description of documents or transactions
1.	A negotiable instrument (a promissory note, bill of exchange other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881). This act applies on Cheque.
2.	A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882).
3.	A trust as defined in section 3 of the Indian Trust Act, 1882 (2 of 1882).
4.	A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called.
5.	Any contract for the sale or conveyance of immovable property or any interest in such property.

[THE SECOND SCHEDULE]

**ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE
AND PROCEDURE**

1. e-authentication technique using Aadhaar [or other] e-KYC services
2. e-authentication technique and procedure for creating and accessing subscriber's signature key facilitated by trusted third party (DSC)
