Toppersnotes®
Unleash the topper in you

Gujarat

Judicial Services Exam

The High Court of Gujarat

Volume - 9

The Information Technology Act 2000, The Protection of Women from Domestic Violence Act 2005, The Immoral Traffic (Prevention) Act 1956, Legal Maxims

SIERRA INNOVATIONS

INDEX

1 CHAPTER The Information Technology Act, 2000

Act No. 21 of 2000,

Date of enforcement: 17th October 2000

Date of enactment: 9th June, 2000

The Act's main purpose is:

1. **To legally recognize electronic transactions**
   - ✓ Earlier, contracts, agreements, and communications had to be on paper and signed physically.
   - ✓ This Act gave **legal validity** to transactions done through **electronic means** like emails, electronic data interchange (EDI), digital signatures, and online communication.
2. **To promote electronic commerce (e-commerce)**
   - ✓ It supports business activities carried out through the internet and other electronic networks.
   - ✓ It allows people and companies to **use digital records instead of paper-based documents**.
3. **To enable e-governance**
   - ✓ Citizens and businesses can file documents, applications, and forms electronically with government agencies.
   - ✓ This reduces dependency on physical paperwork.
4. **To update existing laws**
   - ✓ Since old laws were framed only for paper-based systems, the Act amended:
     - **Indian Penal Code (now BNS)** → to include crimes committed using computers and the internet.
     - **Indian Evidence Act, 1872 (Now BSA)** → to allow **digital evidence** (emails, digital records, etc.) in courts.
     - **Banker's Books Evidence Act, 1891** → to permit banks to keep and produce **electronic records** instead of paper ledgers.
     - **Reserve Bank of India Act, 1934** → to empower RBI to regulate and recognize electronic funds transfer, e-banking, etc.
5. **Other matters connected/incidental**
   - ✓ Covers areas like cybercrime, hacking, data protection, and misuse of electronic records.

CHAPTER - 1

Preliminary

Section 1 – Short Title, Extent, Commencement, and Application

1. **Short Title**
   - ✓ The Act is called the *Information Technology Act, 2000*.
2. **Extent**
   - ✓ It applies to the **whole of India**.
   - ✓ It also applies to **offences or contraventions committed outside India** by any person, provided they involve the provisions of this Act.
3. **Commencement**
   - ✓ The Act comes into force on a date notified by the Central Government.
   - ✓ Different provisions of the Act can come into force on **different dates** (flexibility in implementation).
   - ✓ Any reference to the commencement of the Act in a provision should be interpreted as the commencement date of that specific provision.
4. **Exemptions (Sub-section 4)**
   - ✓ The Act **does not apply** to certain documents or transactions listed in the **First Schedule**.
   - ✓ Examples in the First Schedule include:
     - Negotiable instruments (other than cheques)
     - Powers of attorney
     - Trust deeds
     - Wills and testamentary dispositions
     - Contracts for sale or transfer of immovable property
   - ✓ The **Central Government** has the power to **amend the First Schedule** by adding or deleting entries, via notification in the *Official Gazette*.
5. **Parliamentary Oversight (Sub-section 5)**
   - ✓ Every such notification made under sub-section (4) must be **laid before both Houses of Parliament** for transparency and oversight.

Section 2 – Definitions. – (1) In this Act, unless the context otherwise requires

(a) access with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

First understand the meaning of the two terms grammatical variations and cognate expressions.

1. **Grammatical variations**

   This means the different ways a word or phrase can change depending on grammar rules.
   - Example: The verb "run" changes as "runs, ran, running" → those are grammatical variations.
   - Another example: "child → children" (plural form).

   So basically: same word, different forms depending on tense, number, person, etc.

2. **Cognate expressions**

   "Cognate" means "related" or "having the same origin." Cognate expressions are words or phrases in different languages (or sometimes within the same language) that look or sound similar and often have the same meaning.
   - Example (English & Spanish): "family" and "familia" → they are cognates.
   - Example (English & French): "nation" and "nation."

   So basically: words in different languages that are like cousins because they come from the same root.

   In short:
   - Grammatical variations = different forms of the same word (runs, ran, running).
   - Cognate expressions = similar words across languages (family – familia).

Ingredients of this definition:

1. **Gaining entry** → Entering into a computer system/network (physically or remotely, e.g., logging in).
2. **Instructing** → Giving commands to the system (e.g., executing programs, running codes).
3. **Communicating with resources** → Interaction with the system's **logical, arithmetic, or memory functions**.
   - **Logical functions**: Operations based on logic (e.g., comparisons, conditions).
   - **Arithmetical functions**: Calculations performed by the computer.
   - **Memory functions**: Reading, writing, storing, retrieving data.

   "Access" basically means using or interacting with the internal functions of a computer or network—whether to enter, give instructions, or retrieve/modify data.

Practical Example

- ✓ **Accessing a website** → Communicating with a server.
- ✓ **Running software** → Instructing the logical/arithmetical functions.
- ✓ **Retrieving a file** → Accessing memory resources.
- ✓ **Unauthorized hacking** → Also counts as "access," even if done without permission.

This definition is very broad, it covers both authorized and unauthorized access, which is crucial for offences under the IT Act (e.g., hacking, data theft, unauthorized system entry).

(b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Ingredients:

- ✓ **Addressee** = the person the message (electronic record) is meant for.
- ✓ **Originator** = the person who sends the message.
- ✓ **Intermediary** = someone who just passes the message along (like an email server, internet provider, or a messenger service).

An **addressee** is the *real intended receiver* of the message, **not** the middleman that helps deliver it.

(c) adjudicating officer means an adjudicating officer appointed under sub-section (1) of section 46;

(d) "affixing electronic signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

It means when you sign a physical paper, you use pen to prove "I approve this."

- ✓ In the **digital world**, you "sign" an electronic record using a digital signature, which is a cryptographic method that proves:
  - The document truly comes from you, and
  - It hasn't been altered after you signed it.

Thus, affixing an electronic signature is the digital equivalent of putting your handwritten signature on a physical document.

Ingredients:

"Any methodology or procedure" – It can be any recognized technical process (like asymmetric cryptography, Aadhaar-based e-sign, etc.).

"Authenticating an electronic record" – The purpose is to verify the signer's identity and document integrity.

"By means of digital signature" – The IT Act currently allows only methods that meet the definition of a **digital signature** under the Act (e.g., using a pair of public and private keys issued by a licensed Certifying Authority).

(da) Appellate Tribunal‖ means the Appellate Tribunal referred to in sub-section (1) of section 48;

(e) "Appropriate Government"

This term decides whether the **Central Government** or the **State Government** has authority over a particular matter under the IT Act.

- ✓ **If the matter is under:**
  1. **List II (State List)** of the 7th Schedule → **State Government** is the appropriate government.
  2. **List III (Concurrent List)** but concerning a **State law** → **State Government** again.
- ✓ **In all other cases** (like Union List matters, or general IT-related matters) → **Central Government** is the appropriate government.

Example:

- ✓ Regulation of police communication → State Government (State List).
- ✓ Cyber security policy → Central Government.

(f) "Asymmetric Crypto System"

This is the **technical system behind digital signatures**.

- ✓ It uses **two related keys**:
  1. **Private Key** – used by the sender to create (sign) a digital signature.
  2. **Public Key** – used by others to verify that the signature is genuine.

Example:

When you sign a document digitally, your private key encrypts the hash value; anyone can verify it using your public key.

Ensures both **authenticity** and **integrity** of the message.

(g) "Certifying Authority" (CA)

A **Certifying Authority** is an organization **licensed by the Controller of Certifying Authorities (CCA)** to issue **Digital Signature Certificates (DSCs)** or **Electronic Signature Certificates**.

- ✓ It verifies your identity before issuing a signature certificate.
- ✓ Only approved authorities can legally issue these certificates in India.

Example:

eMudhra, Sify, NIC, and (n)Code Solutions are licensed CAs in India.

(h) "Certification Practice Statement"

It's a formal **document issued by a Certifying Authority** describing how it operates and ensures security.

It specifies:

- ✓ Verification procedures before issuing certificates,
- ✓ How certificates are managed or revoked,
- ✓ Technical and security standards followed.

Example:

Before issuing your DSC, the CA must verify your identity per its **certification practice statement (CPS)**, ensuring reliability.

(ha) "Communication Device"

Added later through an amendment.

Means **any electronic device** used for **sending, receiving, or transmitting** text, video, audio, or images.

Examples:

- ✓ Mobile phones,
- ✓ Tablets,
- ✓ Laptops with communication apps,
- ✓ PDAs (Personal Digital Assistants).

Essentially, **any device used for digital communication**.

(i) "Computer"

A **computer** includes **any high-speed electronic or digital device** that performs logical, arithmetic, or memory operations using electronic, magnetic, or optical impulses.

Includes:

- ✓ CPU, monitor, keyboard (input/output devices),
- ✓ Storage units,
- ✓ Software and communication components connected to it.

Example:

A desktop PC, laptop, or server — all are "computers" under this Act.

(j) "Computer Network"

A **computer network** is a setup where **two or more computers or communication devices are interconnected** for sharing data or resources.

- ✓ Can be connected via:
  - Satellite, microwave, wire, wireless, or any medium.
- ✓ The connection can be continuous or temporary.

Example:

- ✓ Internet,
- ✓ Office LAN (Local Area Network),
- ✓ Wi-Fi-connected systems.

(k) "Computer Resource"

A broad term that includes **everything digital** in a computer ecosystem:

Computer, **Computer system**, **Computer network**, **Database**, **Software**, and **Data**.

Example:

If someone hacks into your e-mail or damages your software, they've tampered with a "computer resource."

(l) "Computer System"

A **computer system** means a **device or group of connected devices** (including input and output devices) that:

- ✓ Contains **computer programs** and **electronic instructions**,
- ✓ Can process **input data** and produce **output data**,
- ✓ Performs functions such as **logical operations, arithmetic operations, data storage, retrieval, and communication control**.

Excludes:

- ✓ **Calculators that are not programmable** (i.e., simple calculators that can't store programs or process external data).

In simple words:

A computer system is a **complete setup** that can **process, store, and communicate information**, not just a single machine.

Examples:

- ✓ Your **desktop computer** connected with a monitor, keyboard, and printer.
- ✓ A **bank's server setup** with terminals and data storage systems.
- ✓ **ATM network system** processing transactions.

(m)"Controller"

"Controller" means the **Controller of Certifying Authorities (CCA)**, appointed under **Section 17(1)** of the IT Act.

Role of the Controller:

- ✓ Supervises and regulates all **Certifying Authorities (CAs)** that issue **digital signature/e-sign certificates**.
- ✓ Ensures **trust, security, and legal compliance** in the digital signature ecosystem.
- ✓ Has power to **suspend or revoke** a CA's license if rules are violated.

Example:

The **Controller of Certifying Authorities (CCA)** under the **Ministry of Electronics and Information Technology (MeitY)** is the national authority for certifying authorities in India.

(na) "Cyber Café"

A **cyber café** is **any public facility** where **internet access is provided** to the public **in the ordinary course of business** (usually for a fee).

Examples:

- ✓ Local computer shops offering internet browsing or printing services.
- ✓ Public browsing centers where people access e-mails, online forms, or social media.

Note:

Under the **IT (Guidelines for Cyber Café) Rules, 2011**, owners must maintain **user identification records** and **system usage logs** for security and traceability.

(nb) "Cyber Security"

Protection of all digital assets — data, devices, computers, networks — from **unauthorized access, misuse, modification, or destruction**.

The purpose is to keep information safe and systems functioning properly.

Example: Firewalls, antivirus software, and encryption used by banks to protect customer data.

(o) "Data"

Any **representation of information or facts** that a computer can process.

It may exist as text, numbers, images, or sound and can be stored in many forms — **printouts, disks, magnetic or optical media, tapes**, etc.

Example: A spreadsheet of exam results or a scanned document stored on a hard drive.

(p) "Digital Signature"

A **method of authenticating an electronic record** using a cryptographic process described in **Section 3** of the IT Act.

It proves:

1. The identity of the sender, and
2. That the document hasn't been altered.
3. **Example:** Signing a PDF using your Digital Signature Certificate (DSC).

(q) "Digital Signature Certificate (DSC)"

An electronic certificate issued under **Section 35(4)** by a licensed **Certifying Authority** to confirm a person's identity for digital transactions.

Example: The DSC you use to sign income-tax or MCA e-forms.

(r) "Electronic Form"

Information that exists or is stored in **digital media**—magnetic, optical, computer memory, microfilm, or similar devices.

Example: A Word file, a scanned image, or a PDF on your computer.

(s) "Electronic Gazette"

The **Official Gazette** of the Government published **digitally** (instead of print).

Example: e-Gazette notifications on government websites.

(t) "Electronic Record"

Covers **all digital data or records**, including text, images, or sounds that are created, sent, received, or stored electronically.

Example: An e-mail, digital photograph, or online transaction log.

(ta)"Electronic Signature"

Any approved **electronic technique** (listed in the Second Schedule) used to authenticate an electronic record — **includes digital signature** but can cover newer methods (like Aadhaar e-sign).

Example: Aadhaar-based e-Sign used on government portals.

(tb)"Electronic Signature Certificate"

A certificate issued under **Section 35** that validates an **electronic signature**, including a **digital signature certificate**.

Example: The certificate behind your e-Sign authentication.

(u) "Function" (of a Computer)

Refers to all operations a computer can perform — **logic, arithmetic, deletion, storage, retrieval, and communication**.

Example: A computer calculating totals, deleting a file, or sending an e-mail.

(ua) "Indian Computer Emergency Response Team (CERT-In)"

An agency created under **Section 70B(1)** to act as the **national nodal agency for cyber-security incidents**.

Example: CERT-In handles hacking, phishing, and malware attack alerts in India.

(v) "Information"

Includes **data, messages, text, images, sound, voice, software, databases**, or any content stored in digital or microfilm form.

Example: A WhatsApp message or a database of voter records.

(w) "Intermediary"

Any person or company that **receives, stores, transmits, or provides a service** for another person's electronic records.

Includes **telecom operators, ISPs, web-hosting sites, search engines, payment gateways, e-commerce platforms**, and even cyber cafés.

Example: YouTube, Amazon, or Airtel — they act as intermediaries between users.

(x) "Key Pair"

A matched set of two mathematically linked keys in **asymmetric cryptography**:

- ✓ **Private Key** → used to create a digital signature.
- ✓ **Public Key** → used to verify it.
- ✓ **Example:** The pair used when you digitally sign a document.

(y) "Law"

Covers **all valid legal instruments** — Acts of Parliament or State Legislatures, Ordinances, Presidential Regulations, President's Acts under Art. 357, and any rules, bye-laws, or orders made under them.

(z) "Licence"

The official **authorization granted under Section 24** to a **Certifying Authority** to issue digital/e-signature certificates.

(za) "Originator"

The **person who creates or sends an electronic message** to another person, but **not an intermediary**.

Example: If you send an e-mail, you are the originator; Gmail is only the intermediary.

(zb) "Prescribed"

Means specified or laid down by **rules made under this Act** by the appropriate government.

(zc) "Private Key"

The **secret part** of a key pair used to **create a digital signature**.

It must be kept confidential by the owner.

Example: When you sign an e-file, your private key encrypts the document's digital hash.

(zd) "Public Key"

- ✓ It is the **second part of a key pair** in an asymmetric crypto system.
- ✓ The **public key** is used to **verify a digital signature** that was created using the corresponding **private key**.
- ✓ This key is **listed in the Digital Signature Certificate (DSC)** issued to a subscriber.

Example:

When you digitally sign a file with your private key, others can check its authenticity using your public key (which is publicly available through your DSC).

(ze) "Secure System"

A system (hardware, software, and procedures) that meets all these conditions:
(a) It is **reasonably safe** from unauthorized access or misuse.
(b) It works **reliably and correctly**.
(c) It is **fit for its intended purpose**.
(d) It **follows accepted security standards and practices**.

Example:

An e-governance portal that uses encryption, access control, and audit logs is a **secure system**.

(zf) "Security Procedure"

Refers to the **security measures prescribed by the Central Government under Section 16** of the Act.

These ensure the integrity, confidentiality, and authenticity of electronic records and signatures.

Example: Rules for digital signature verification or encryption standards notified by MeitY.

(zg) "Subscriber"

A **person in whose name an electronic-signature or digital-signature certificate is issued**.

This person is legally responsible for the use of the private key linked to that certificate.

Example:

If you obtain a DSC from eMudhra, **you** are the subscriber.

(zh) "Verify" (Check)

In relation to a **digital signature**, **electronic record**, or **public key**, "verify" means to check:

(a) Whether the electronic record was signed using the **private key** corresponding to the subscriber's **public key**; and
(b) Whether the record has remained **intact and unaltered** since the digital signature was applied.

Example:

When someone opens your digitally signed PDF, their computer uses your public key to verify that the file was indeed signed by you and not changed afterward.

Sub-section (2): Reference to Corresponding Law

If this Act mentions any **law or enactment** that is **not in force in a particular area**, it should be understood as referring to the **corresponding law in force in that area**.

Purpose:

To make the IT Act applicable even in regions where a particular central or state enactment is not yet operational, by linking it to an equivalent law there.

CHAPTER - 2

Digital Signature and Electronic Signature

Section 3: Authentication of Electronic Records

(1) Authentication by Digital Signature

- ✓ Any **subscriber** (the person to whom a digital-signature certificate has been issued) can **authenticate an electronic record** by **affixing his digital signature** to it.
- ✓ This digital signature serves the same purpose as a **handwritten signature** on a physical document — it confirms the sender's identity and intent.

Example:

When you digitally sign an income-tax return (ITR) form before uploading it online, you are authenticating it under Section 3(1).

(2) How Authentication Works — Asymmetric Crypto System + Hash Function

The authentication process uses two core technologies:

(a) Asymmetric Crypto System

- ✓ Involves a **key pair**:
  - A **private key** (known only to the subscriber) — used to **sign** the document.
  - A **public key** (accessible to everyone) — used to **verify** the signature.

(b) Hash Function

- ✓ A **mathematical algorithm** that converts any electronic record into a **unique fixed-length string** called a **hash value** (or "hash result").
- ✓ The digital signature is applied to this hash, not to the full document — making the process secure and efficient.

Purpose of the Hash Function:

1. The same input always gives the **same hash result**.
2. It is **computationally infeasible** to:
   (a) Reconstruct the original file from its hash, or
   (b) Find two different files with the same hash result (collision-free).

Example:

If you digitally sign a PDF, a hash value of that PDF is first created → your private key encrypts that hash → the receiver uses your public key to decrypt and check the hash → if the hashes match, authenticity and integrity are confirmed.

(3) Verification Using the Public Key

- ✓ Anyone can verify the authenticity of a digital signature by using the **public key** of the subscriber.

- ✓ If the decrypted hash (from the signature) matches the recomputed hash (from the document), it proves:
- ✓ The document was signed by the rightful owner, and
- ✓ The document hasn't been changed since signing.

(4) Uniqueness of Key Pair

- ✓ Each subscriber has a **unique pair** of **private and public keys**.
- ✓ Together, they form a **functioning key pair** for secure communication and authentication.

Section 3A – Electronic Signature

This section extends authentication beyond *digital* signatures to include **any reliable electronic authentication technique** approved by the Government.

(1) Use of Electronic Signature

- ✓ Even if Section 3 talks about *digital signatures*, a subscriber may instead use **any electronic signature or authentication technique** that—
  (a) is **considered reliable**, and
  (b) is **listed in the Second Schedule** of the Act.

Thus, both *digital* and other *electronic* signatures (like Aadhaar e-Sign) are legally valid.

(2) When an Electronic Signature Is "Reliable"

An electronic signature is deemed **reliable** only if it meets all these five conditions

Clause	Requirement	Meaning in Simple Words
(a)	Signature / authentication data are linked uniquely to the signatory	The signature must belong to one identifiable person only
(b)	Signature data were under the signatory's exclusive control when signing	No one else could have used or accessed the signing key
(c)	Any alteration to the electronic signature after signing is detectable	Tampering with the signature can be discovered
(d)	Any change in the signed data after authentication is detectable	The system will show if the document was edited post-signature
(e)	Meets other prescribed technical / security standards	Central Govt can add extra reliability conditions

If these are satisfied, the signature is *legally trustworthy* and admissible as proof of identity and consent.

(3) Verification Procedure

- ✓ The **Central Government** may **prescribe the procedure** to verify whether an electronic signature truly belongs to the claimed person.
- ✓ This ensures a uniform national verification process (e.g., Aadhaar-based OTP or biometric check).

(4) Updating the Second Schedule

- ✓ The **Central Government** can, through notification in the **Official Gazette**,
  - **add or remove** an electronic-signature method, and
  - specify the **procedure** for affixing it.
- ✓ **Proviso:** No technique may be added unless it is proven *reliable* under clause (2).

(5) Parliamentary Oversight

- ✓ Every such Government notification must be **laid before both Houses of Parliament**, ensuring democratic scrutiny.

Illustration

Situation	Example
Government-approved e-signature	**Aadhaar e-Sign** (OTP or biometric-based) used for Income-Tax filings
Reliable features	Unique to user, controlled by user, detects alteration, traceable
Authority adding new method	MeitY (Central Govt) via Gazette notification updates the Second Schedule

This section gives legal recognition to all **reliable electronic authentication methods**, not just digital signatures.

It ensures **security, exclusivity, and tamper detection**, with Government control over approval and verification procedures.

CHAPTER - 3

Electronic Governance

Section 4 – Legal Recognition of Electronic Records

If any law requires something to be **"in writing"**, **typewritten**, or **printed**, that requirement is satisfied when:

1. the information is **available in electronic form**, and
2. it is **accessible and usable later** for reference.

Meaning: Digital documents (PDFs, e-mails, etc.) are legally valid equivalents of written documents.

Section 5 – Legal Recognition of Electronic Signatures

Where the law requires a **signature** on a document, the requirement is met if the document is **authenticated by an electronic signature** affixed as per Central Government rules.

Explanation: "Signed" includes any handwritten mark; hence, an electronic signature is its legal digital counterpart.

Example: A digitally signed income-tax return is valid like a physically signed paper form.

Section 6 – Use of Electronic Records and Signatures in Government

Government agencies may accept and issue documents **electronically** for:

- filing forms or applications,
- granting licences or approvals,
- receiving or paying money.

The **appropriate Government** can make rules prescribing:

- the **format/method** of electronic filing or issue,
- the **manner of paying fees** electronically.

Example: Online passport applications and e-payment of licence fees.

Section 6A – Delivery of Services by Service Provider

- Government can **authorise private or public service providers** (like CSCs, private IT firms) to deliver public services electronically.
- Such providers can **collect service charges**, as notified.
- The Government must publish in the **Official Gazette** the scale of permissible charges.

Example: Common Service Centres (CSCs) collecting small e-service fees for PAN, Aadhaar, or certificates.

Section 7 – Retention of Electronic Records

If any law requires documents to be **retained for a specific period**, that requirement is met when they are kept electronically, **provided that**:
(a) information stays **accessible** for later use,
(b) the record's **format remains authentic or demonstrably accurate**,
(c) **origin, destination, date, and time** details are recorded.

Purpose: Ensures that electronic archiving has the same validity as physical record-keeping.

Section 7A – Audit of Electronic Documents

If any law requires **audit** of documents or records, the same rule applies to those **maintained electronically**.

Example: Digital accounting records can be legally audited like paper ledgers.

Section 8 – Publication in Electronic Gazette

Any rule, regulation, or notification that must be published in the **Official Gazette** is validly published if released **electronically**.

- The **date of publication** is the date of whichever version—print or electronic—appears first.

Example: e-Gazette notifications on government websites are legally recognised.

Section 9 – No Right to Insist on Electronic Form

Sections 6–8 do **not** give individuals a right to demand that government offices **must** accept or issue documents electronically.

Acceptance of e-records is **optional** for the department concerned.

Section 10 – Power to Make Rules for Electronic Signatures

The **Central Government** can make rules on:
(a) types of electronic signatures,
(b) their format and manner of affixation,
(c) identification of the signatory,
(d) security and confidentiality procedures, and
(e) any other matter needed to give legal effect to e-signatures.

Example: Rules for Aadhaar-based e-Sign authentication.

Section 10A – Validity of E-Contracts

Contracts formed through **electronic communication** (e-mail, website click-wrap, etc.) are **legally valid and enforceable**.

They cannot be rejected merely because they were made electronically.

Example: Online shopping orders or e-banking agreements have full contractual validity.

CHAPTER - 4

Attribution, Acknowledgment and Despatch of Electronic Records

Section 11 – Attribution of Electronic Records

This section explains **who is considered the sender ("originator")** of an electronic record.

An electronic record will be treated as sent **by the originator** if:

1. **He sent it himself**, or
2. **Someone authorised** by him sent it on his behalf, or
3. It was sent **automatically by a computer system** that he or his agent programmed.

Example:

If a company's automated billing software sends e-mails to customers, those e-mails are legally considered to be sent by the company.

Section 12 – Acknowledgment of Receipt

This section deals with how the **receiver ("addressee") confirms receipt** of an electronic record.

(1) How acknowledgment can be given

If the sender hasn't specified a particular way to acknowledge, the receiver may confirm receipt by:

- ✓ any **communication** (manual or automated), or
- ✓ any **action** showing that the message has been received (like replying or downloading it).

Example:

If you send an invoice by e-mail and the recipient replies "Received," that's an acknowledgment.

(2) When acknowledgment is required for validity

If the sender has clearly stated that the electronic record is **binding only after acknowledgment**,

then —if the acknowledgment is **not received**, the record is treated as **never sent**.

Example:
A supplier's e-mail says, "This order is valid only after you acknowledge receipt."
If no acknowledgment comes, the order doesn't legally exist.

(3) If acknowledgment isn't received in time

If no special condition is mentioned and the acknowledgment doesn't arrive within:

- ✓ the **agreed time**, or
- ✓ a **reasonable time**,

then the sender can:

1. **Notify** the receiver that acknowledgment hasn't been received,
2. Give a **deadline** to respond, and
3. If still not received, treat the record as **never sent**.

Example:

A company sends a digital proposal. If the client doesn't acknowledge even after a reminder, the sender can legally consider it void

Section 13 – Time and Place of Dispatch and Receipt

This section defines **when** and **where** an electronic record is considered sent and received.

(1) Time of Dispatch

- ✓ A message is **dispatched** when it **leaves the sender's control** — i.e., when it enters another computer system (like an e-mail server).

Example:

An e-mail is dispatched when it leaves your outbox and reaches your e-mail service provider's server.

(2) Time of Receipt

(a) If the receiver has a **designated system** for such messages:
  (i) It's received when it **enters that system**, or
  (ii) If sent elsewhere, when the receiver **retrieves it**.

(b) If no system is designated, it's received when it **enters the receiver's computer**.

Example:

If a company has a special inbox for "orders@abc.com", the order is received once it reaches that inbox.

(3) Place of Dispatch and Receipt

Unless agreed otherwise:

- ✓ A record is **deemed dispatched** from the sender's **place of business**,
- ✓ And **deemed received** at the receiver's **place of business**.

This rule applies even if the actual computer system is located somewhere else (like on a cloud server).

(4) Place Definitions

- ✓ If multiple business places → the **main (principal)** place counts.
- ✓ If no business → the **usual residence** counts.
- ✓ For companies → the **registered office** is treated as the usual residence.

CHAPTER - 5

Secure Electronic Records and Secure Electronic Signature

Section 14 – Secure Electronic Record

Meaning:

If an electronic record (like a file, email, or database entry) has had a **security procedure** properly applied to it at a particular time, it is legally treated as a **secure electronic record from that point onward until it is verified.**

In simple words:

A digital document becomes *secure* once an approved security method (like encryption, hash locking, or digital signature) has been applied to it — and it stays secure unless tampered with.

Example:

If an e-contract is digitally signed and encrypted at 10:00 a.m., it is considered a **secure record** from 10:00 a.m. until verification.

Section 15 – Secure Electronic Signature

Meaning:

An electronic signature is treated as a **secure electronic signature** if it meets two key conditions:

1. The **signature creation data** (e.g., private key, password, biometric data)
2. was **under the exclusive control of the signatory** at the time of signing.
3. (No one else could access or use it.)
4. The signature data was **stored and affixed in an exclusive, prescribed manner** —
5. i.e., using government-approved secure hardware or software procedures.

Explanation:
For digital signatures, "**signature creation data**" means the **private key** of the subscriber — this private key must be secure and confidential.

Example:
If you use your personal DSC (Digital Signature Certificate) stored on a token device, and only you can access it via your password or PIN → your signature is a **secure electronic signature**.

Section 16 – Security Procedures and Practices

Meaning:

The **Central Government** is empowered to make rules specifying **how** security procedures and practices should be followed for:

- **Secure electronic records (Section 14)** and
- **Secure electronic signatures (Section 15).**

While making these rules, the Government must consider:

- The **nature of commercial transactions**,
- The **level of risk**, and
- **Practical business circumstances**.

Example:

The Government (through MeitY) prescribes technical standards — like encryption algorithms, secure storage methods, or digital-signature validation protocols — to ensure uniform cybersecurity practices.

CHAPTER - 6

Regulation of Certifying Authorities

Section 17 – Appointment of Controller and Other Officers

- The **Central Government** appoints the **Controller of Certifying Authorities (CCA)** through the *Official Gazette*.
- It may also appoint **Deputy Controllers, Assistant Controllers, and staff**.
- The Controller works **under the general direction of the Central Government**.
- Deputies/Assistants act under the **supervision of the Controller**.
- The Government fixes their **qualifications, service terms**, and **office locations**.
- The Controller's Office has an **official seal**.

Example:

The present CCA under the Ministry of Electronics and IT (MeitY) supervises all licensed Digital Signature Certifying Authorities in India.

Section 18 – Functions of Controller

The Controller performs key regulatory and supervisory duties, including:

1. **Supervising Certifying Authorities (CAs)**.
2. **Certifying public keys** of CAs.
3. **Laying down standards** for security and operations.
4. Setting **employee qualifications** for CAs.
5. Specifying **business conditions** and advertising rules.
6. Defining **form/content of electronic-signature certificates**.

7. Regulating **account formats and audit rules**.
8. Allowing CAs to create **joint electronic systems**.
9. Settling **disputes between CAs and subscribers**.
10. Maintaining a **public database** of every CA's disclosure record.

Purpose: Ensures uniform security, transparency, and public trust in India's digital signature infrastructure.

Section 19 – Recognition of Foreign Certifying Authorities

- The Controller (with Central Government approval) may **recognise foreign CAs** by notification.
- Their e-signature certificates then become **legally valid in India**.
- Recognition can be **revoked** if conditions are violated.

Example: Recognition of an overseas CA for cross-border trade or banking transactions.

Section 20 – Controller to Act as Repository (omitted)

This earlier section was **deleted by the 2008 Amendment** because the repository function was reassigned to CAs and the Controller's database.

Section 21 – Licence to Issue Electronic Signature Certificates

- Anyone may apply to the Controller for a **licence to act as a Certifying Authority**.
- The applicant must have adequate **technical expertise, staff, financial capacity and infrastructure**.
- Licence is:
  - ✓ valid for a prescribed period,
  - ✓ **non-transferable**, and
  - ✓ subject to regulations.

Section 22 – Application for Licence

Must include:

1. **Certification Practice Statement (CPS)**,
2. **Procedure for verifying applicant identity**,
3. **Fee (up to ₹25,000)**, and
4. Other prescribed documents.

Section 23 – Renewal of Licence

This section lays down the **procedure for renewing the licence** of a **Certifying Authority (CA)** — the entity authorised to issue digital or electronic signature certificates.

Key Ingredients:

1. **Form of Application:**
   - ✓ The renewal application must be submitted **in the prescribed form**, as defined by the **Central Government** through rules.
2. **Application Fees:**
   - ✓ The application must be accompanied by a **fee**, which can be **up to ₹5,000** (maximum limit prescribed).
3. **Time Limit:**
   - ✓ The application must be made **at least 45 days before** the **expiry date** of the current licence.

Purpose:

- ➢ To ensure **continuous and uninterrupted functioning** of Certifying Authorities.
- ➢ To give the **Controller of Certifying Authorities (CCA)** adequate time to review and renew the licence before it expires.

Example

If a Certifying Authority's licence is set to expire on **30 June 2026**, it must apply for renewal **on or before 16 May 2026** (i.e., 45 days earlier), using the prescribed form and fee.

Section 24 – Grant or Rejection of Licence

- ➢ Controller may **grant or reject** the application after scrutiny.
- ➢ **Rejection requires a hearing** ("reasonable opportunity to present the case").

Section 25 – Suspension or Revocation of Licence

Licence may be **revoked/suspended** if a CA:

(a) gave false information,
(b) breached licence conditions,
(c) failed to maintain required standards, or
(d) violated any law / rule.

- ✓ Temporary suspension (max 10 days) is allowed pending inquiry.
- ✓ A suspended CA cannot issue new e-signature certificates.

Section 26 – Notice of Suspension or Revocation

- ➢ Controller must **publish the notice online** in its database and all repositories.
- ➢ The information must be **accessible 24×7** on a website.

Section 27 – Power to Delegate

The Controller can **authorise Deputy / Assistant Controllers** to exercise specific powers in writing.