# Cyber Authorities

| |
|---|
| **Controller, deputy controller, assistant controller** |
| **Certifying authority** |
| **Adjudicating Officer** |
| **Cyber Appellate tribunal**<br>• **Constitution**<br>• **Jurisdiction**<br>• **Powers and Procedure** |
| **Subscriber** |
| **Intermediary** |
| **Computer Emergency Response Team** |

### ❖ Controller, deputy controller, assistant controller-

According to Sec 17 of the IT Act the Central government is empowered to appoint a Controller of Certifying authorities.

The organizational structure of Controller of Certifying authorities is as follows-

- Minister of Electronics and IT
- Minister of State (E & IT)
- Secretary
- Controller of Certifying Authority
- Deputy controller
- Assistant Controller
- Technical Officer

**Functions of Controller—**

Since 2000, the office of Controller of Certifying authorities has 3 broad functions-

1- Technology
2- Finance and Legal
3- Investigation

(Each department has a Deputy controller and an Assistant Controller).

According to IT Act, 2000, the controller has following functions-

(a) exercising supervision over the activities of the Certifying Authorities;
(b) certifying public keys of the Certifying Authorities;
(c) laying down the standards to be maintained by the Certifying Authorities;
(d) specifying the qualifications and experience which employees of the Certifying Authority should possess;
(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a electronic signature Certificate and the public key;

(g) specifying the form and content of a electronic signature Certificate and the key;
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
(m) laying down the duties of the Certifying Authorities;
(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Section 28 of the Act provides that, the Controller or any officer authorized by him shall have power to investigate contraventions as laid down in the provisions of this Act. The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the Certifying Authorities in the country.

### ❖ Certifying authority-

Certifying Authority means a person who has been granted a licence to issue a electronic signature Certificate under section 24. The IT Act 2000 gives details of who can act as a CA. Accordingly a prospective CA has to establish the required infrastructure, get it audited by the auditors appointed by the office of Controller of Certifying Authorities, and only based on complete compliance of the requirements, a license to operate as a Certifying Authority can be obtained. The license is issued by the Controller of Certifying Authority, Ministry of Information Technology.

The Controller of Certifying Authorities (CCA) has established the Root Certifying Authority (RCAI) of India under section 18(b) of the IT Act to digitally sign the public keys of Certifying

Authorities (CA) in the country. The RCAI is operated as per the standards laid down under the Act.

### ❖ Adjudicating Officer-

Adjudicating officer (AO)AO is appointed under section 46 of the IT Act to adjudicate offences under Chapter IX.

As per Rule 3 of the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003, it has been declared that the Secretary of Department of Information Technology of every State and Union Territory shall serve as Adjudicating officer.

Important sections regarding AO under the IT Act –

- Section 46 – Power to adjudicate
- Section 47 – Factors to be taken into account by the adjudicating officer

### ❖ Cyber Appellate tribunal-

Cyber Appellate Tribunal has been established under the Information Technology Act under the aegis of Controller of Certifying Authorities (C.C.A.).

According to Sec 2 (da) ―Appellate Tribunal- means the Appellate Tribunal referred to in sub-section (1) of section 48. The first and the only Cyber Appellate Tribunal in the country has been established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.

#### ➢ Constitution of Cyber Appellate tribunal–

A Cyber Appellate Tribunal shall consist of one person only (the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

- A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he-

(a) is, or has been, or is qualified to be, a Judge of a High Court;or;

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

- Staff of the Cyber Appellate Tribunal:

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officer and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

- **Jurisdiction of Cyber Appellate tribunal**

Appeal to Cyber Appellate Tribunal:

- Any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal jurisdiction in the matter.
- No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
- 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 as prescribed.
- Right to legal representation- The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.
- Civil court not to have jurisdiction - No court shall have jurisdictions to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Appeal to High Court:

- Any person aggrieved by any decision or order of the Cyber 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 Cyber Appellate Tribunal to him on any question of fact or law arising out of such order.
- The High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

➢ **Procedure & Power**

- The Cyber Appellate Tribunal is not bound by the procedure laid down by the Code of Civil Procedure, 1908.
- But, it shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, i.e. : -
    (a) summoning and enforcing the attendance of any person and examining him on oath;
    (b) requiring the discovery and production of documents or other electronic records;
    (c) receiving evidence on affidavits;
    (d) issuing commissions for the examination of witnesses of documents;
    (e) reviewing its decisions;
    (f) dismissing an application for default or deciding it ex parte;
    (g) any other matter which may be prescribed.
- It shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules.
- The Tribunal shall also have powers to regulate its own procedure including the place at which it shall have its sitting.
- Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purpose of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

### ❖ Subscriber-

As defined under Sec 2 (zg) subscriber means a person in whose name the electronic signature Certificate is issued.

Duties of Subscriber (Sections 40-41) include-

- Generating the key pair (the public and the private key) in case of digital certificate.
- Retaining control of the private key corresponding to the public key listed in his Digital Signature Certificate with reasonable care, ensuring it is not disclosed.
- If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.
- The subscriber is required to accept the digital signature by authorizing the publication of same to one or more persons or in a repository in any other manner.

### ❖ Intermediary-

Sec 2 (w) defines as any person who on behalf of another person receives, stores or transmits any electronic record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

### ❖ Computer Emergency Response Team

ICERT is a national nodal agency for responding to computer security incidents and has been empowered so under Sec 70B of IT Act.

It is the only authority for issue of instructions in the context of blocking websites. CERT-IN, after verifying the authenticity of the complaint and after satisfying that action of blocking of the website is absolutely essential, instructs Department of Telecommunication (DoT)-Latest

Release (LR Cell) to block the website. DoT, under whose control the Internet Service Providers (ISPs) are functioning will ensure the blocking of websites and inform CERT-IN accordingly.

Functions of CERT-

1- Collection, analysis, dissemination of information on cyber incidents.
2- Forecast and alerts of cyber security incidents
3- Coordination of cyber response activities
4- Issue guidelines, whitepapers etc relating to information security practices, procedures, prevention, response, reporting cyber crimes.