The IT Act accommodates the Controller of Certifying Authorities(CCA) to permit and direct the working of Certifying Authorities. The Certifying Authorities (CAs) issue computerized signature testaments for electronic confirmation of clients. The Controller of Certifying Authorities (CCA) has been named by the Central Government under Section 17 of the Act for reasons for the IT Act. The Office of the CCA appeared on November 1, 2000. It targets advancing the development of E-Commerce and E-Governance through the wide utilization of computerized marks.

The Controller of Certifying Authorities (CCA) has set up the Root Certifying Authority (RCAI) of India under segment 18(b) of the IT Act to carefully sign the open keys of Certifying Authorities (CA) in the nation. The RCAI is worked according to the gauges set down under the Act. The CCA guarantees the open keys of CAs utilizing its own private key, which empowers clients in the internet to confirm that a given testament is given by an authorized CA. For this reason it works, the Root Certifying Authority of India (RCAI). The CCA likewise keeps up the Repository of Digital Certificates, which contains all the authentications gave to the CAs in the nation.

Role of Certifying Authorities:

Certificate Authority (CA) is a confided in substance that issues Digital Certificates and open private key sets. The job of the Certificate Authority (CA) is to ensure that the individual allowed the extraordinary authentication is, truth be told, who the individual in question professes to be.

The Certificate Authority (CA) checks that the proprietor of the declaration is who he says he is. A Certificate Authority (CA) can be a confided in outsider which is answerable for genuinely confirming the authenticity of the personality of an individual or association before giving an advanced authentication. A Certificate Authority (CA) can be an outer (open) Certificate Authority (CA) like verisign, thawte or comodo, or an inward (private) Certificate Authority (CA) arranged inside our system. Certificate Authority (CA) is a basic security administration in a system. A Certificate Authority (CA) plays out the accompanying capacities. A Controller plays out a few or the entirety of the following roles:

1. Administer the exercises of the Certifying Authorities and furthermore confirm their open keys.
2. Set out the guidelines that the Certifying Authorities follow.
3. Determine the accompanying capabilities and furthermore experience necessities of the workers of all Certifying Authorities conditions that the Certifying Authorities must follow for directing business the substance of the printed, composed, and furthermore visual materials and ads in regard of the advanced mark and the open key the structure and substance of an advanced mark declaration and the key the structure and way where the Certifying Authorities look after records terms and conditions for the arrangement of examiners and their compensation.

4. Encourage the Certifying Authority to set up an electronic framework, either exclusively or together with other Certifying Authorities and its guideline.
5. Indicate the way where the Certifying Authorities manage the endorsers.
6. Resolve any irreconcilable situation between the Certifying Authorities and the endorsers.
7. Set out the obligations of the Certifying Authorities.
8. Keep up a database containing the revelation record of each Certifying Authority with all the subtleties according to guidelines. Further, this database is open to the general population.