



SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution



Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT, Cyber Security including Blockchain Technology)

19SB623 – ETHICAL HACKING AND CYBER LAWS

III YEAR₁/ VI SEMESTER

UNIT 2 – REGULATION TO CYBERCRIMES

TOPIC 1 - Regulating Certifying Authorities.

2/14/2025



The role & function of certifying authorities

- Certificate Authority is a trusted entity that issues Digital Certificates and Public-private Key pairs.
- The role of the Certificate Authority is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.
- A certificate authority is a trusted entity that issues electronic documents that verify a digital entity's identity on the internet.
- The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important role in the public key infrastructure(PKI)



Features of Certifying Authorities

- The certificate Authority verifies that the owner of the certificate is who he says he is.
- A certificate authority can be a trusted third party which is responsible for physically verifying the legitimacy of the identity of an individual or organisation before issuing a digital certificate
- A Certifying Authority can be an external (public) Certifying Authority like Verisign, Thawte or comodo, or an internal (private) Certificate Authority configured inside our network.



Functions of a certifying Authority

- Certifying Authority is a critical security service in a network.
- A Certificate Authority performs the following functions.
- **Certificate Authority Verifies the Identity:**
 - *The Certificate Authority must validate the identity of the entity who requested a digital certificate before issuing it.*
- **Certificate Authority issues digital certificates:**
 - *Once the validation process is over, the Certificate Authority issues the digital certificate to the entity who requested it.*
 - *Digital certificate can be used for encryption (example: Encryption web traffic), code signing, authentication etc.,*



Functions of a certifying Authority

- *Certificate Authority maintains Certificate Revocation List*
 - The Certificate Authority maintains Certificate Revocation List.
 - A certificate revocation list is a list of digital certificates which are no longer valid and have been revoked and therefore should not be relied by anyone.



Exercising supervision over the activities of the Certifying authorities.

Certifying public keys of the Certifying Authorities

Laying down the standards to be maintained by the Certifying Authorities

Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

Specifying Authorities shall conduct their business specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature and the Public Key.

Specifying the form and content of a Electronic Signature Certificate and the key.



Specifying the form and manner, in which accounts shall be maintained by the Certifying Authorities.

Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.

Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

shall conduct their dealings with the subscribers;

Resolving any conflict of interests between the Certifying Authorities and the subscribers;

Laying down the duties of the Certifying Authorities;
Maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars, as may be subjected to conditions.



THANK YOU