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)

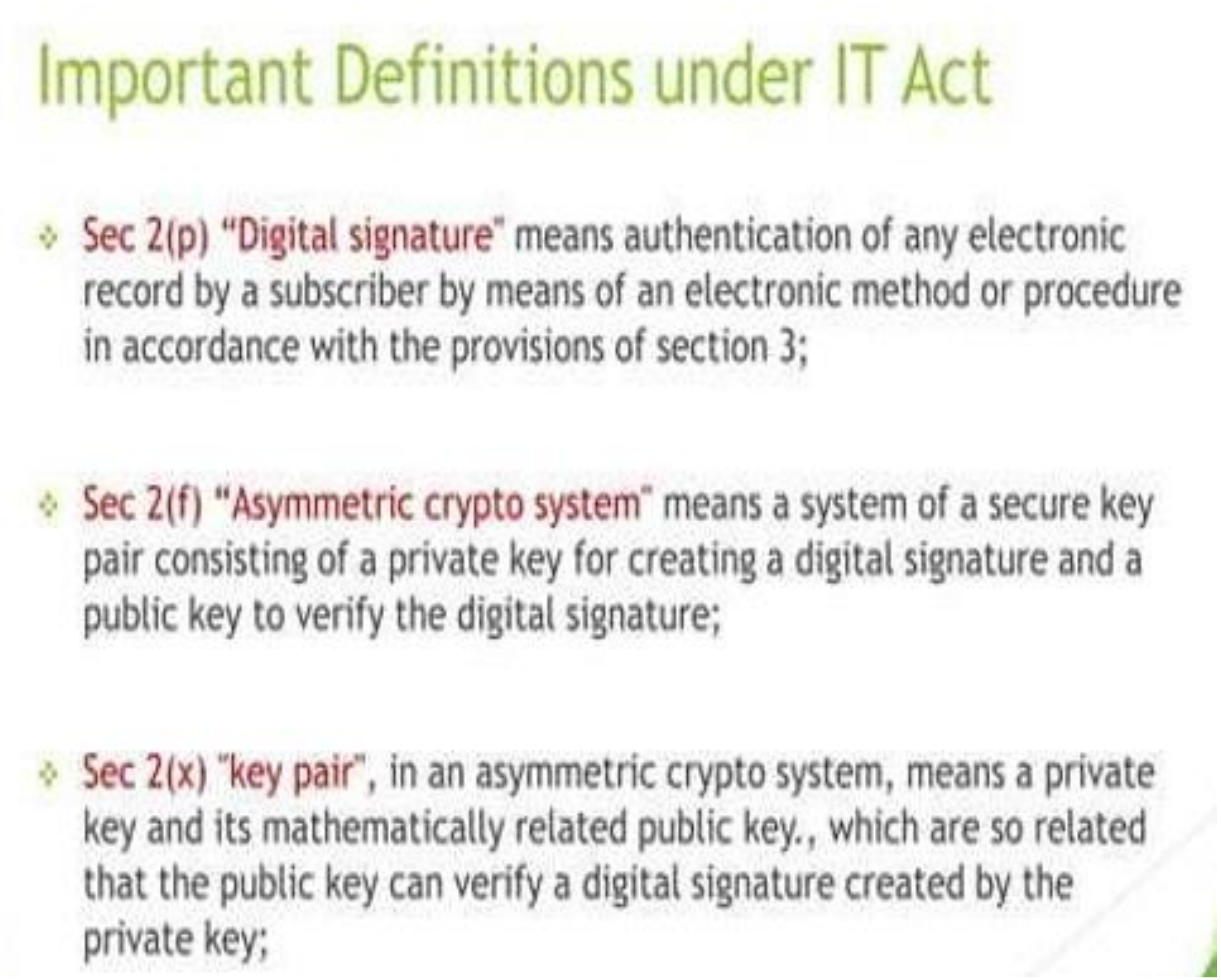
19SB623 – ETHICAL HACKING AND CYBER LAWS

III YEAR/ VI SEMESTER

UNIT 2 – REGULATION TO CYBERCRIMES

TOPIC 4 – Digital Signature / Electronic Signature

Technology of Digital Signatures in India

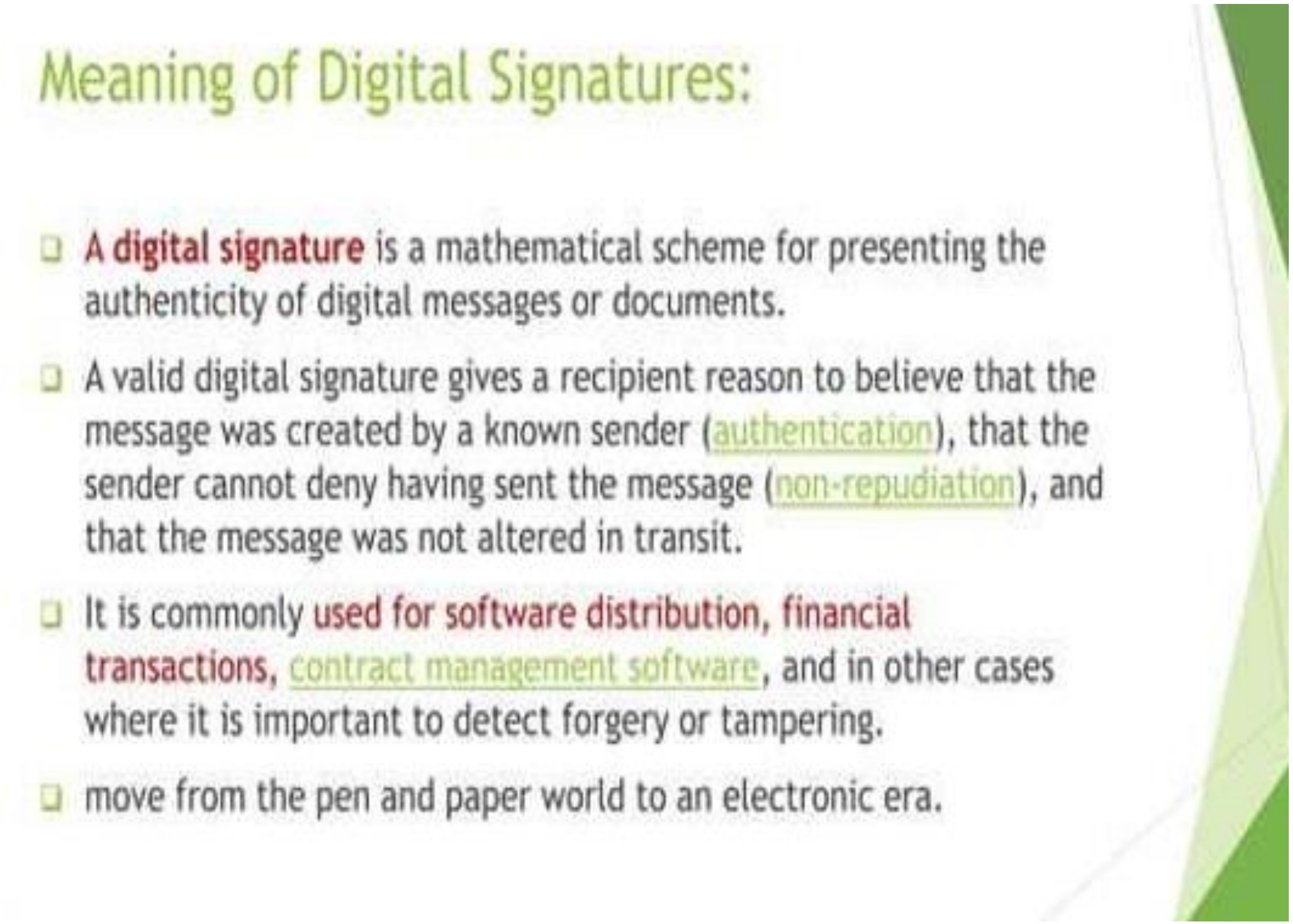


Important Definitions under IT Act

- Sec 2(p) "Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

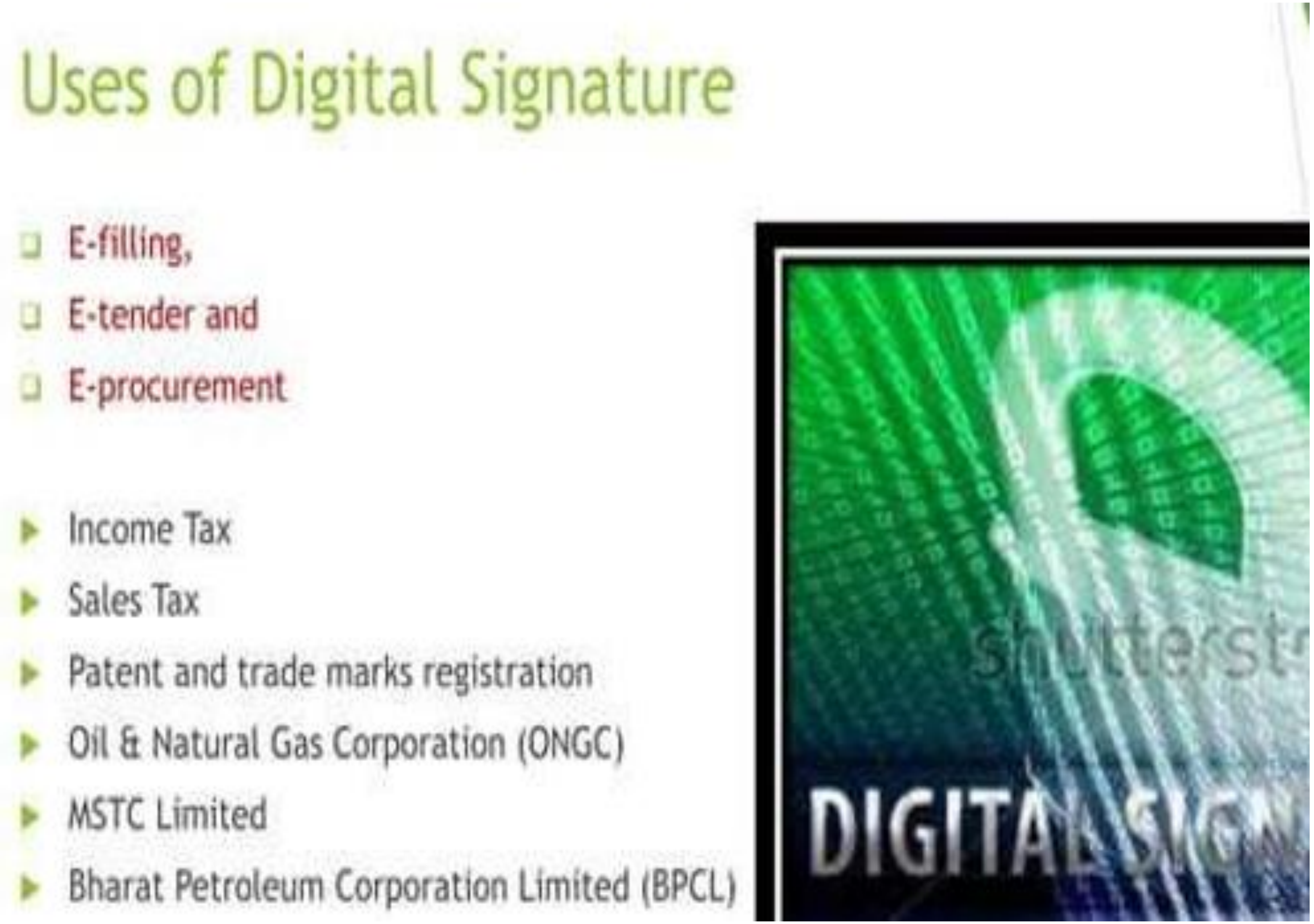
- Sec 2(f) "Asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

- Sec 2(x) "key pair", in an 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;



Meaning of Digital Signatures:

- □ A **digital signature** is a mathematical scheme for presenting the authenticity of digital messages or documents.
- □ A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit.
- □ It is commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.
- □ move from the pen and paper world to an electronic era.

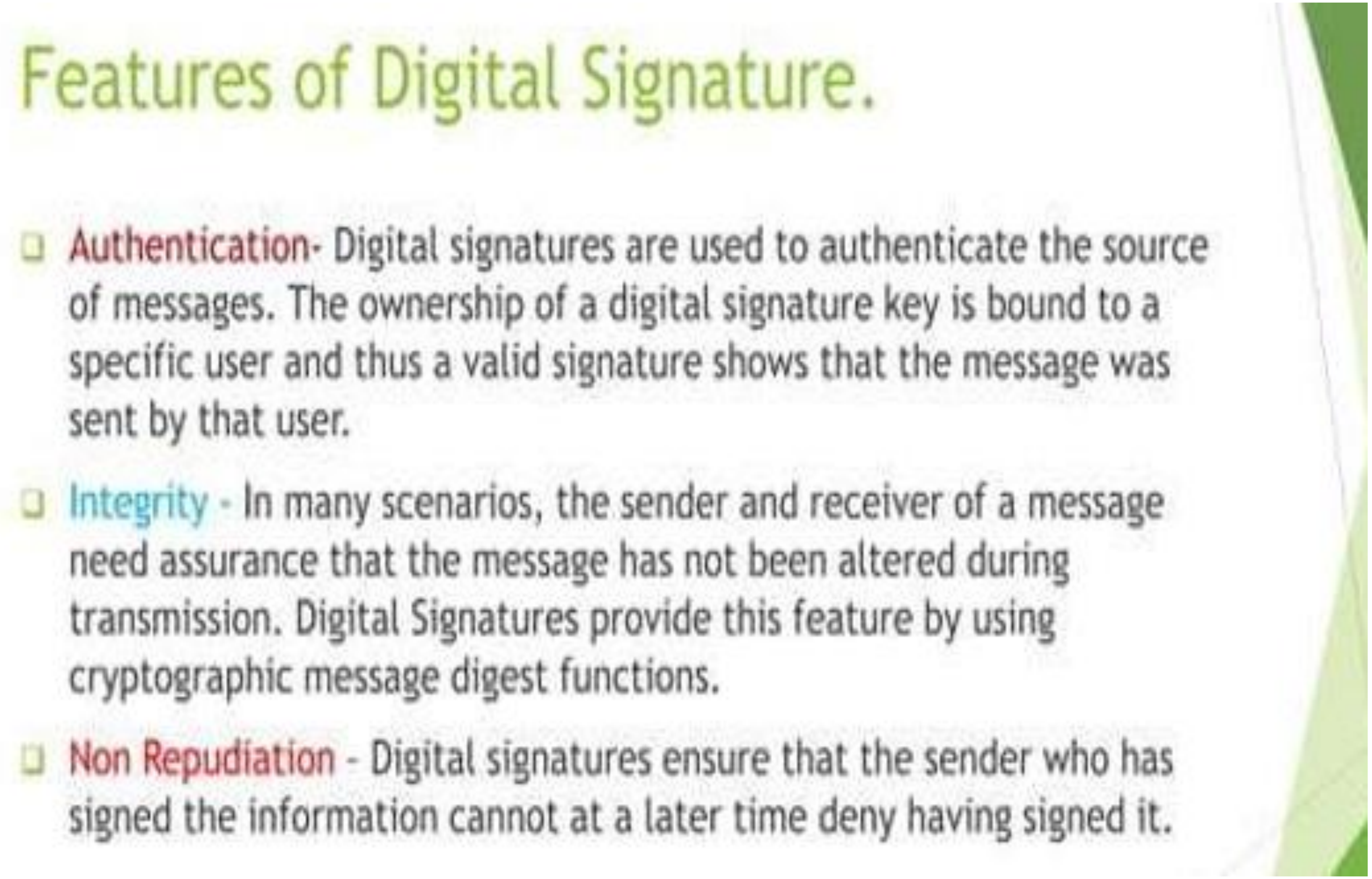


Uses of Digital Signature

- E-filling,
- E-tender and
- E-procurement

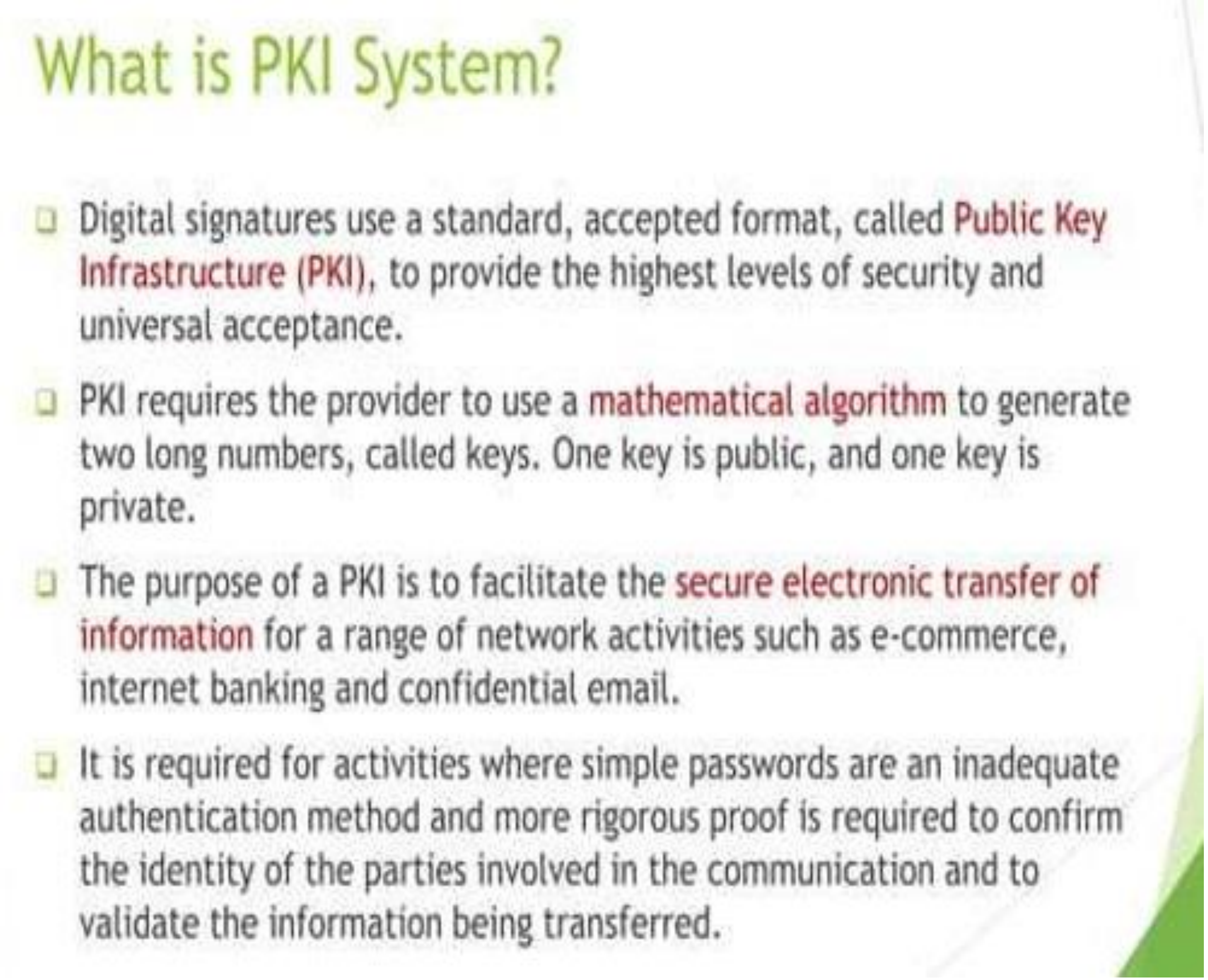
- Income Tax
- Sales Tax
- Patent and trade marks registration
- Oil & Natural Gas Corporation (ONGC)
- MSTC Limited
- Bharat Petroleum Corporation Limited (BPCL)

DIGITAL SIGN



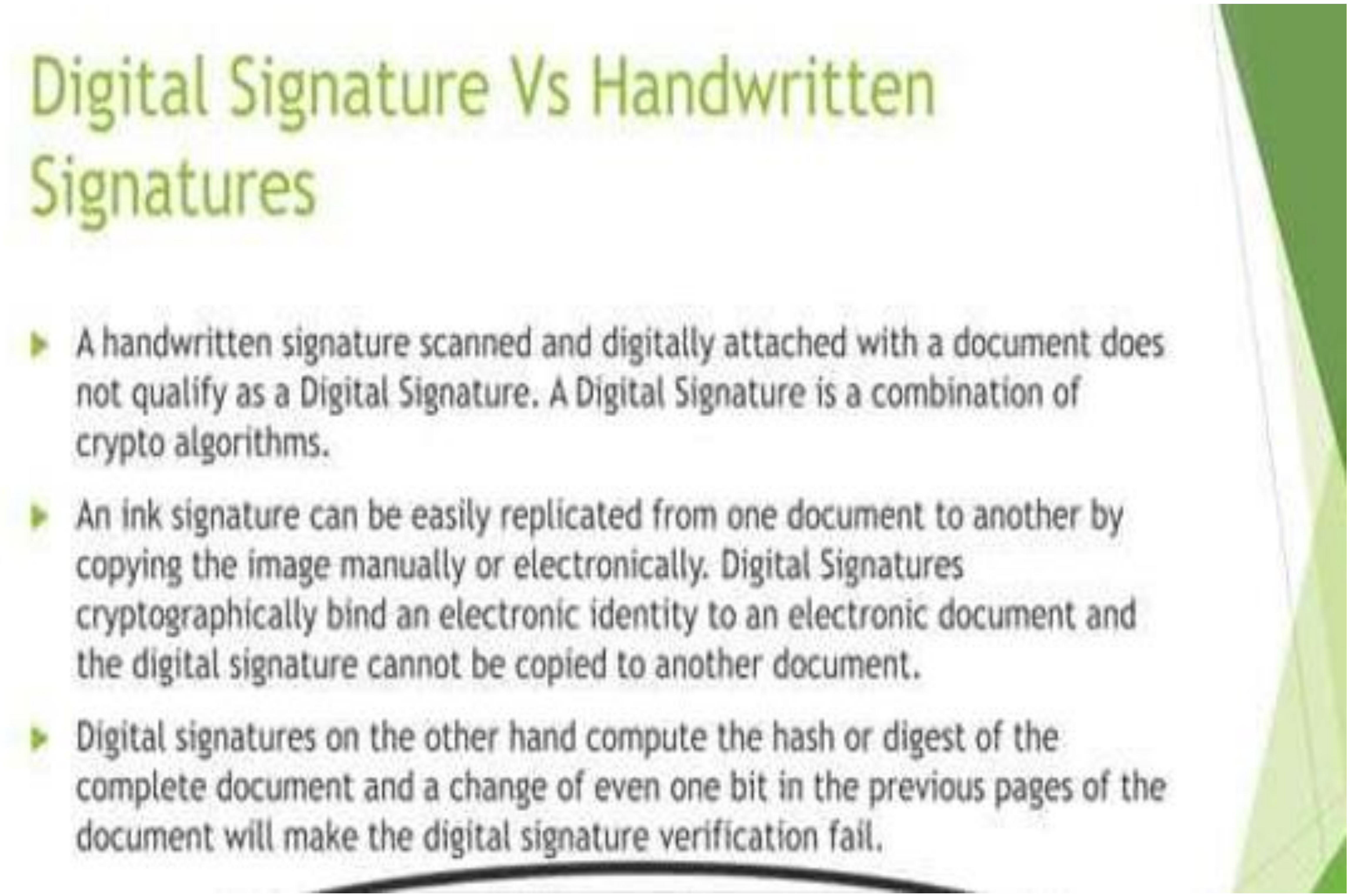
Features of Digital Signature.

- □ Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.
- □ Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions.
- □ Non Repudiation - Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.



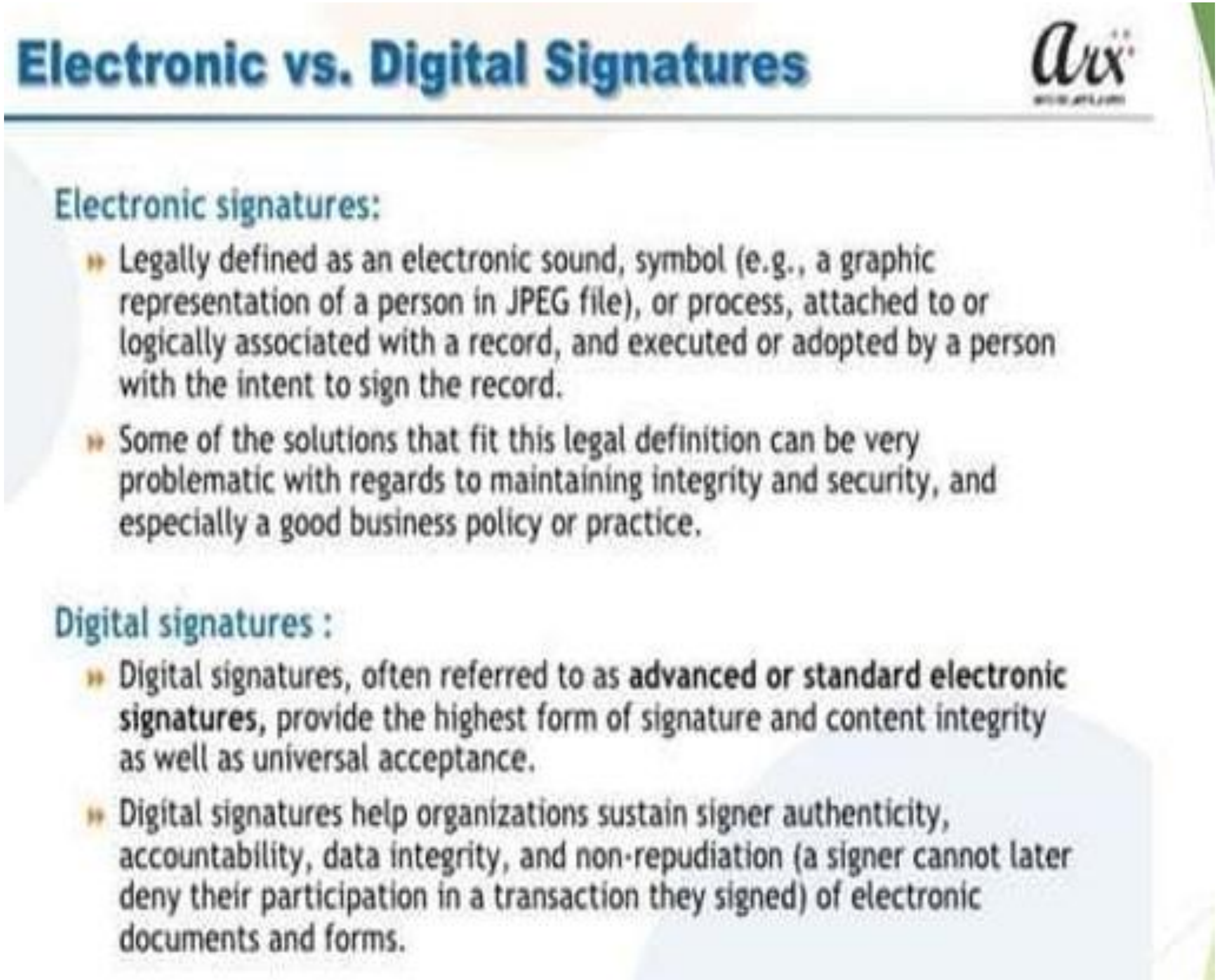
What is PKI System?

- Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance.
- PKI requires the provider to use a mathematical algorithm to generate two long numbers, called keys. One key is public, and one key is private.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
- It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.



Digital Signature Vs Handwritten Signatures

- A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. A Digital Signature is a combination of crypto algorithms.
- An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document.
- Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail.



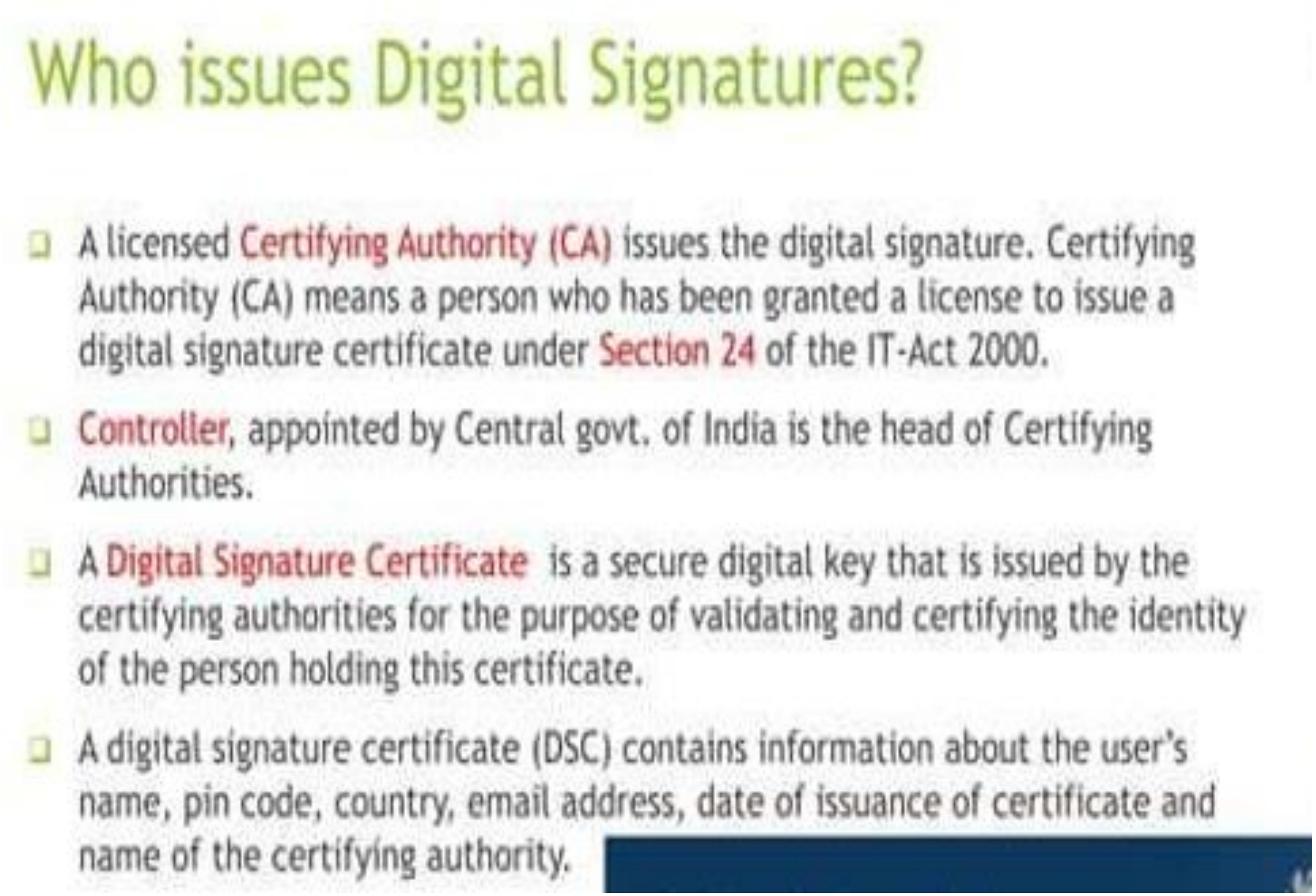
Electronic vs. Digital Signatures

Electronic signatures:

- Legally defined as an electronic sound, symbol (e.g., a graphic representation of a person in JPEG file), or process, attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record.
- Some of the solutions that fit this legal definition can be very problematic with regards to maintaining integrity and security, and especially a good business policy or practice.

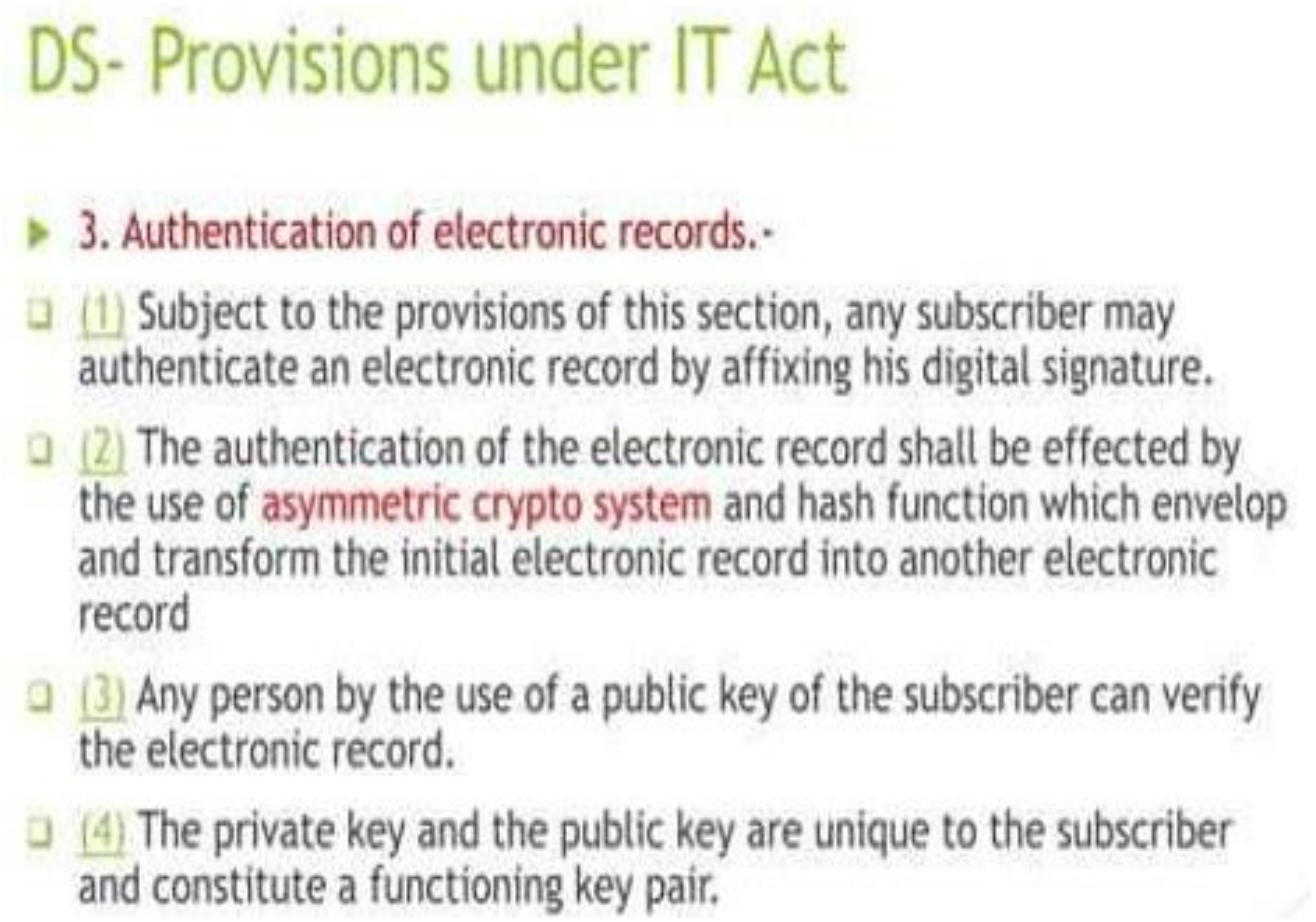
Digital signatures :

- Digital signatures, often referred to as **advanced or standard electronic signatures,** provide the highest form of signature and content integrity as well as universal acceptance.
- Digital signatures help organizations sustain signer authenticity, accountability, data integrity, and non-repudiation (a signer cannot later deny their participation in a transaction they signed) of electronic documents and forms.



Who issues Digital Signatures?

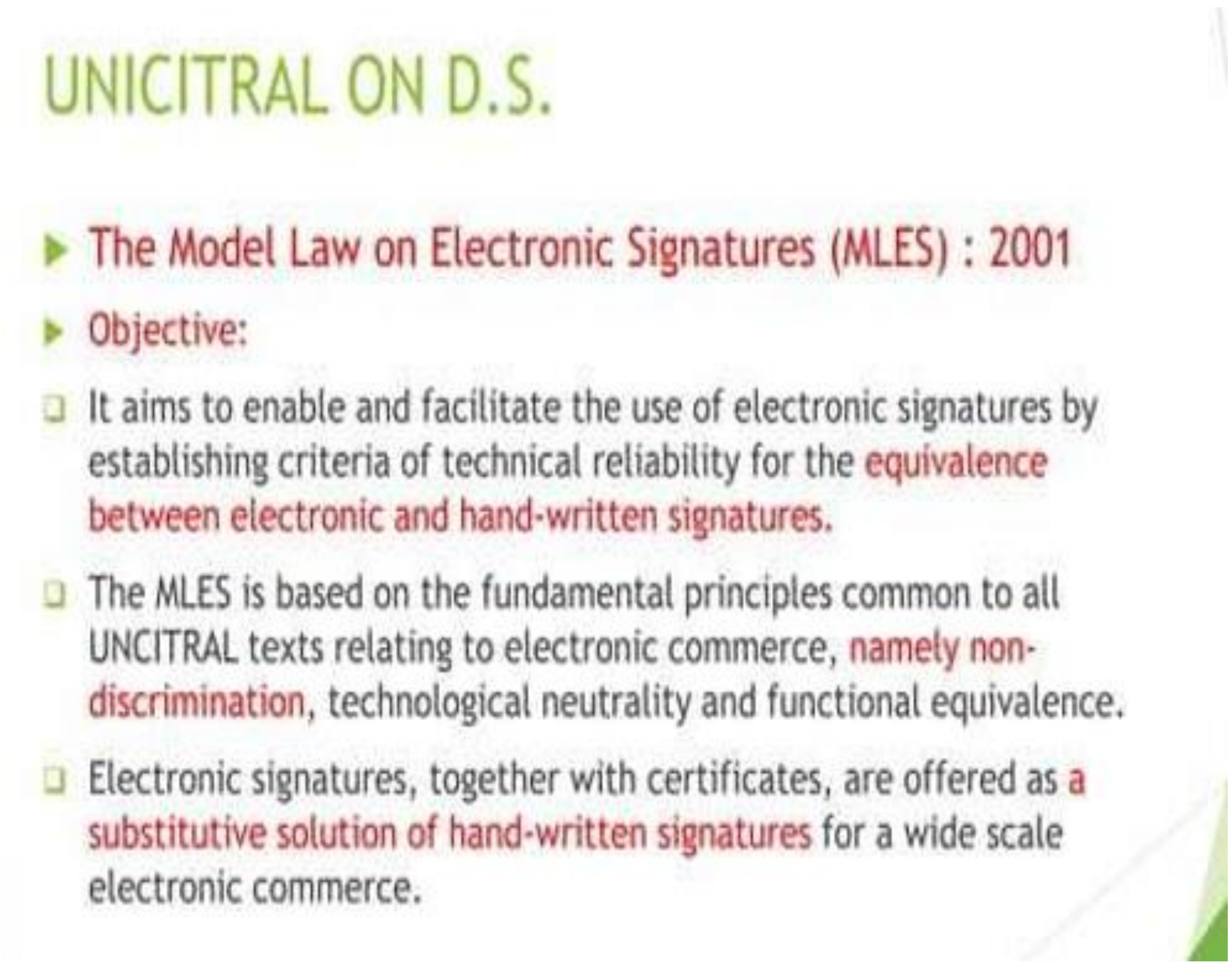
- ❑ A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a license to issue a digital signature certificate under Section 24 of the IT-Act 2000.
- ❑ Controller, appointed by Central govt. of India is the head of Certifying Authorities.
- ❑ A Digital Signature Certificate is a secure digital key that is issued by the certifying authorities for the purpose of validating and certifying the identity of the person holding this certificate.
- ❑ A digital signature certificate (DSC) contains information about the user's name, pin code, country, email address, date of issuance of certificate and name of the certifying authority.



DS- Provisions under IT Act

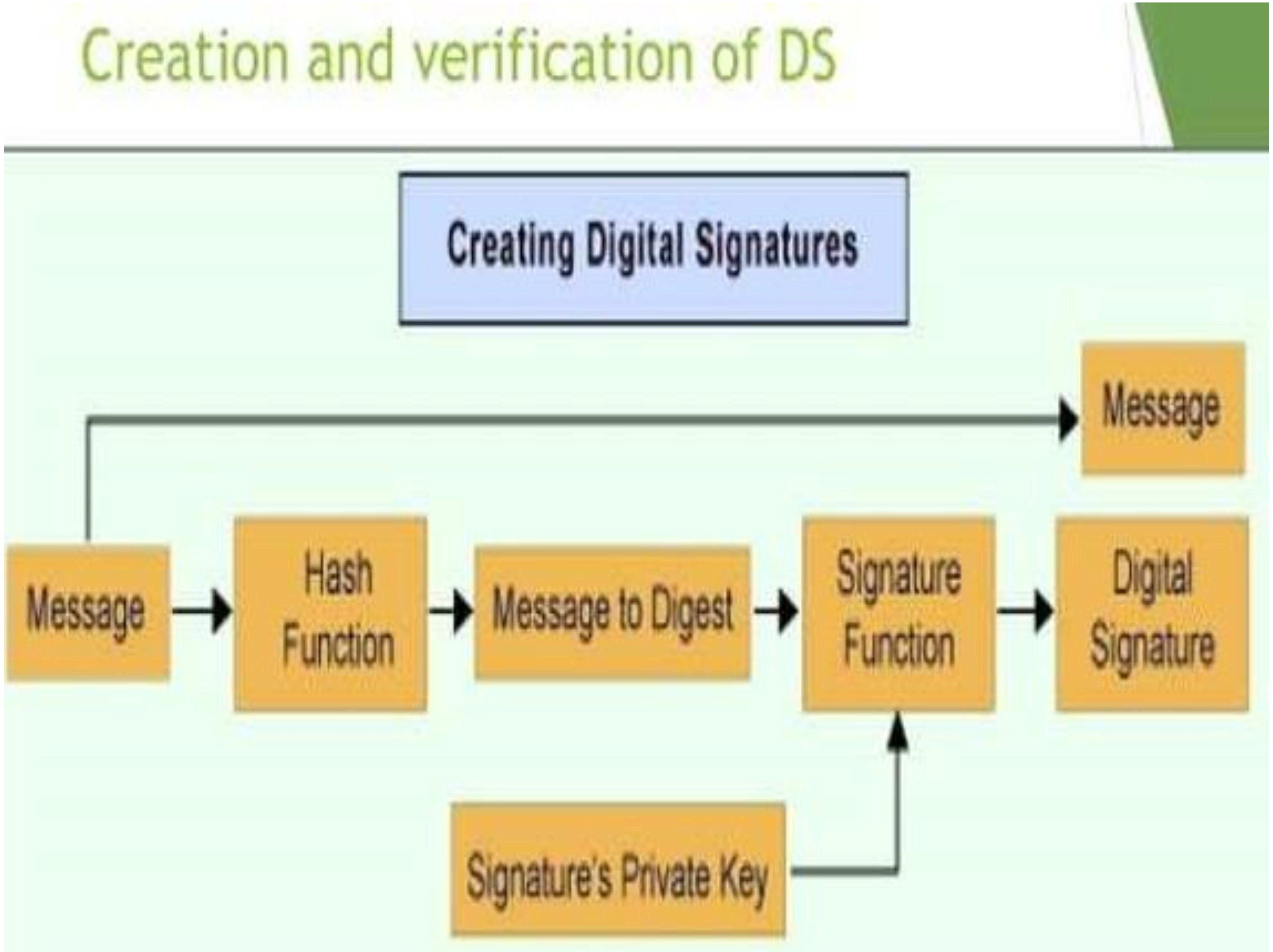
- 3. Authentication of electronic records.-

- (1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.



UNICITRAL ON D.S.

- The Model Law on Electronic Signatures (MLES) : 2001
- Objective:
  - It aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures.
  - The MLES is based on the fundamental principles common to all UNCITRAL texts relating to electronic commerce, namely non-discrimination, technological neutrality and functional equivalence.
  - Electronic signatures, together with certificates, are offered as a substitutive solution of hand-written signatures for a wide scale electronic commerce.



Creation and verification of DS

Creating Digital Signatures

Message

Message

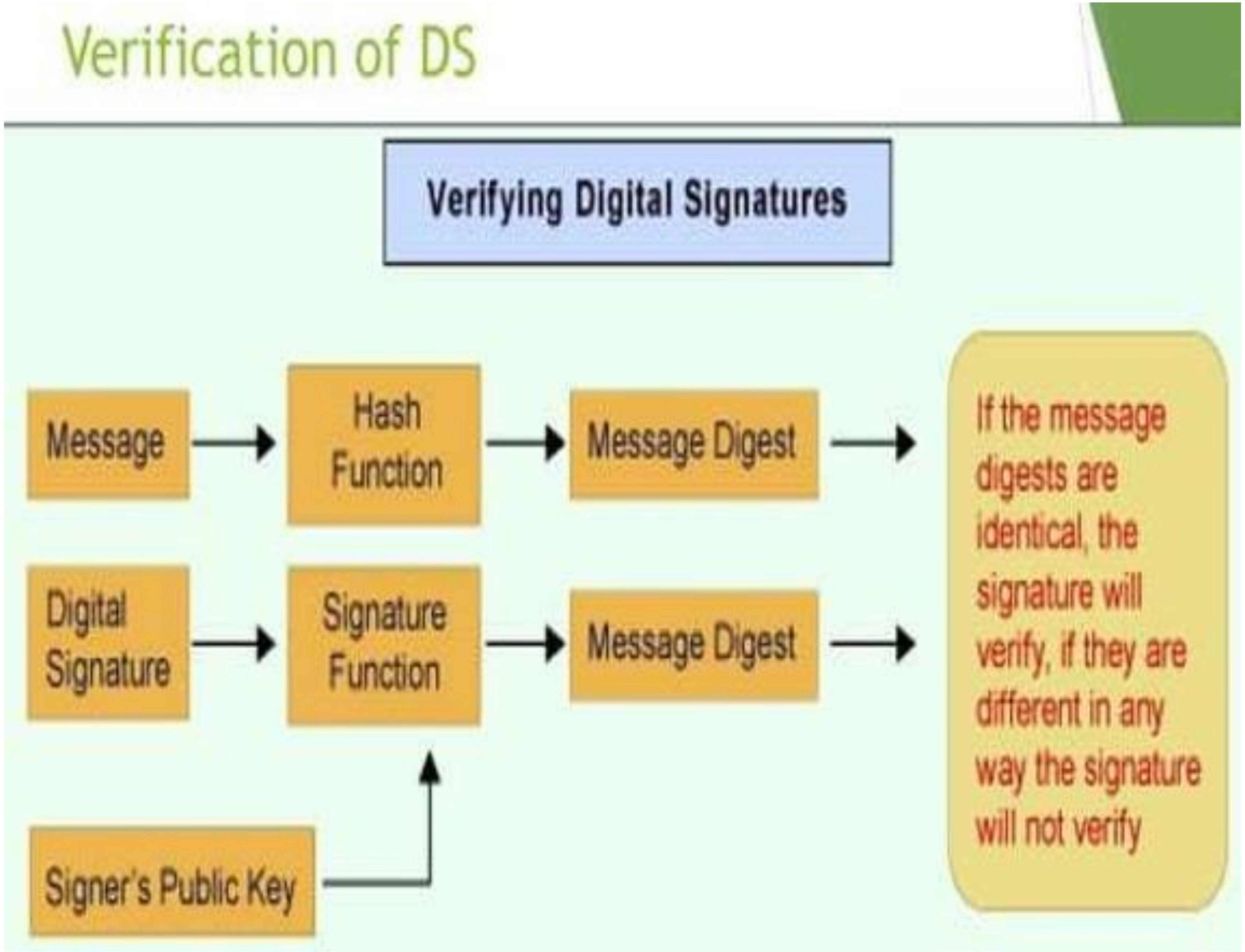
Hash Function

Message to Digest

Signature Function

Digital Signature

Signature's Private Key



Verification of DS

Verifying Digital Signatures

Message → Hash Function → Message Digest →

Digital Signature → Signature Function → Message Digest →

Signer's Public Key → Signature Function

If the message digests are identical, the signature will verify, if they are different in any way the signature will not verify

THANK YOU