SNS COLLEGE OF ENGINEERING
Kurumbapalayam(Po), Coimbatore – 641 107
An Autonomous Institution
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

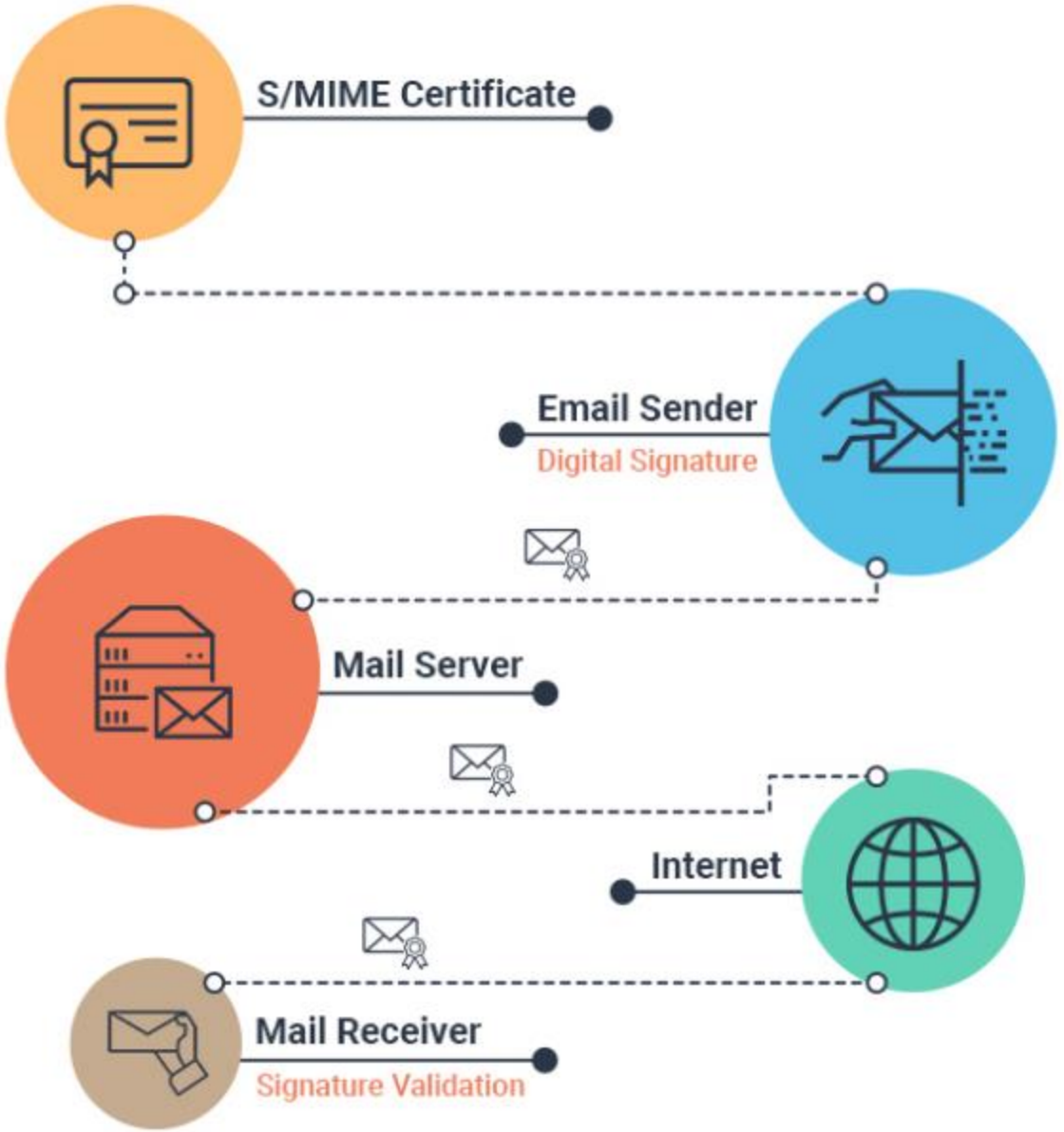
Unit 5: CYBER SECURITY SAFEGUARDS AND SECURITY SERVICES

Topic : S/MIME

S/MIME

- Secure/Multipurpose Internet Mail Extensions

How it works?


S/MIME Certificate
Email Sender
Digital Signature
Mail Server
Internet
Mail Receiver
Signature Validation

Applications

from:	**onlinecourses@nptel.iitm.ac.in**
reply-to:	noc19-mg60-announce+owners@nptel.iitm.ac.in
to:	noc19-mg60-announce@nptel.iitm.ac.in
date:	Oct 4, 2019, 7:50 PM
subject:	Feedback for Design Thinking - A Primer
mailing list:	noc19-mg60-announce@nptel.iitm.ac.in Filter messages from this mailing list
mailed-by:	nptel.iitm.ac.in
signed-by:	nptel-iitm-ac-in.20150623.gappssmtp.com
security:	Standard encryption (TLS) Learn more
:	Important according to Google magic.

Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

- Hash functions: SHA-1 & MD5
- Digital signatures: DSS & RSA
- Session key encryption: ElGamal & RSA
- Message encryption: Triple-DES, RC2/40 and others
- Have a procedure to decide which algorithms to use

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- Managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- Each client has a list of trusted CA's certs
- And own public/private key pairs & certs
- Certificates must be signed by trusted CA's

Thank You