SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

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 ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit II- E-MAIL SECURITY & FIREWALLS

Topic : S / MIME

INTRODUCTION

S/MIME stands for Secure/Multipurpose Internet Mail Extensions.

Through encryption, S/MIME offers protection for business emails.

S/MIME is a protocol used for encrypting or decrypting digitally signed E-mails. This means that users can digitally sign their emails as the owner(sender) of the e-mail.

Emails could only be sent in NVT 7-bit format in the past, due to which images, videos, or audio were not a part of e-mail attachments.

S/MIME is an upgrade of MIME(Multipurpose Internet Mail Extensions

E-Mail Formats

- **RFC5322** – Basic format of an email

- **RFC 2045** – MIME (**Support for Different Content Types:** Text, images, audio, video, and other binary data and a**ttachments:** Enables sending files along with the email body.
- **RFC2046 -**
  - Defines the general structure of the different MIME media types.
  - Introduces **primary content types**, such as:
  - text – Plain text, HTML.
  - image – JPEG, PNG, GIF.
  - audio – MP3, WAV.

- **RFC 2047 - MIME Header Extensions for Non-ASCII Text**
  - Extends email headers (like Subject, From, and To) to include **non-ASCII characters**.
  - Important for supporting international characters in headers.

SMTP

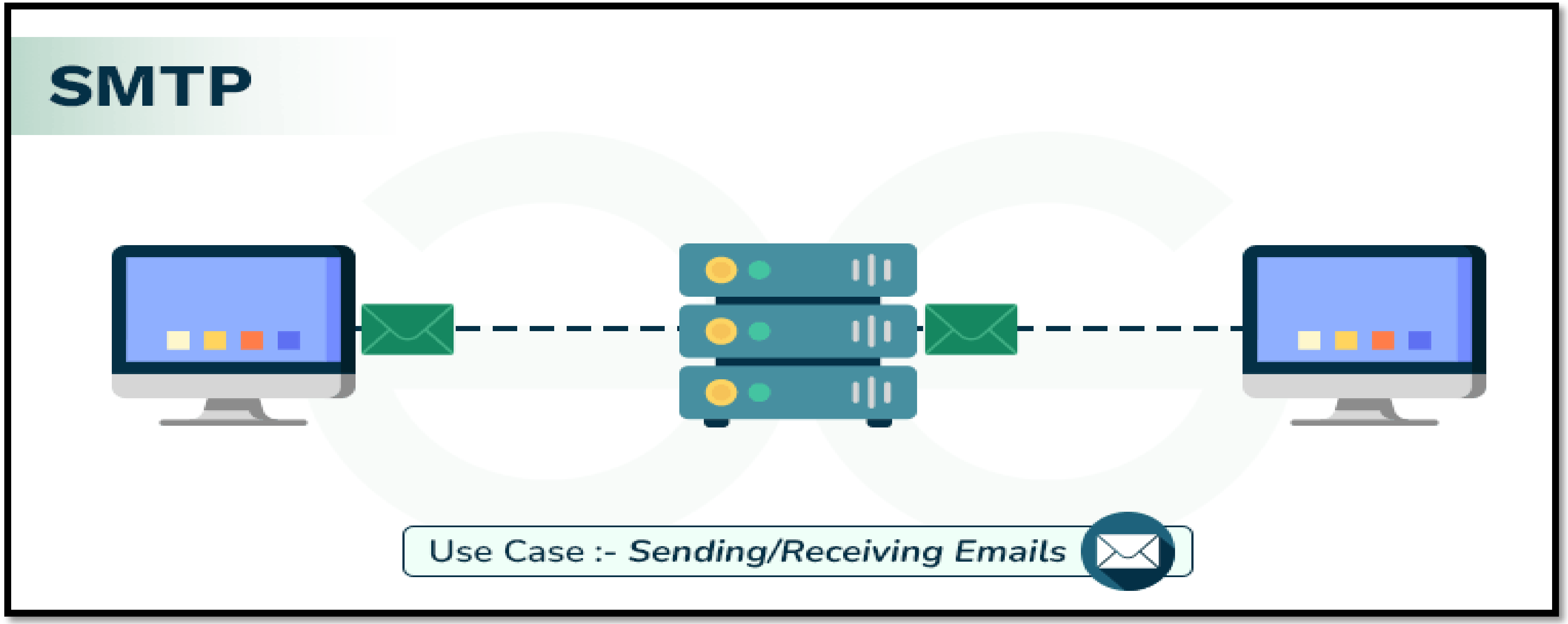
- Simple Mail Transfer mechanism (SMTP) is a mechanism for exchanging email messages between servers. SMTP is an application layer protocol.
- The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection.
- The SMTP server is an always-on listening mode.
- As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.
- It is an essential component of the email communication process and operates at the application layer of the TCP/IP protocol stack. SMTP is a protocol for transmitting and receiving email messages

SMTP

SMTP Protocol

The SMTP model is of two types:

- End-to-End Method - is used to communicate between different organizations
- Store-and-Forward Method – is used within an organization



S/ MIME CERTIFICATIONS

- S/MIME certificates are essential components of the S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol, providing encryption, authentication, and integrity to email communications.
- It is A **digital certificate** that Contains
  - a user's public key.
  - Is issued by a **Certificate Authority (CA)**.
  - Verifies the identity of the certificate holder.
- Essential for:
  - **Encrypting** emails.
  - Adding **digital signatures** to emails.

- Key Components
  - **Public Key:** Used for encrypting messages.
  - **Digital Signature:** Ensures the sender's authenticity.
  - **Issuer Information:** Details of the CA that issued the certificate.
  - **Validity Period:** Certificate start and end dates.
  - **Serial Number:** Unique identifier for the certificate.
  - **Subject:** The entity (person or organization) to whom the certificate is issued.

S/MIME CERTIFICATE

Key Features of SMIME Certificate

•Industry-standard for public key encryption (asymmetric encryption) for MIME-based data.

•Offers two key email security functionalities — digital signatures and encryption.

•Digital signatures provide message integrity, authentication.

•Encryption provides data confidentiality (both for in-transit and at-rest data).

- S/MIME uses asymmetric public key infrastructure (PKI), it employs two keys mathematically associated with each other to facilitates email security.

By digitally signing your emails, the intended recipient can verify that the message was actually sent by you and hasn't been tampered with or modified.

When the email is en route from your computer to the recipient's device, data encryption ensures that any attacker over the wire can't read the contents of the message.

How to Get S/MIME Certificates

Choose a Certificate Authority: You can select any trusted Certificate Authority, such as Sectigo, DigiCert, or GlobalSign, that has the functionality to provide you with S/MIME certificates.

Get or Apply for a Certificate: Log on to the website of the CA, and select the S/MIME certificate you would like to buy or apply for. You might be asked for your name, email address, and organizational details.

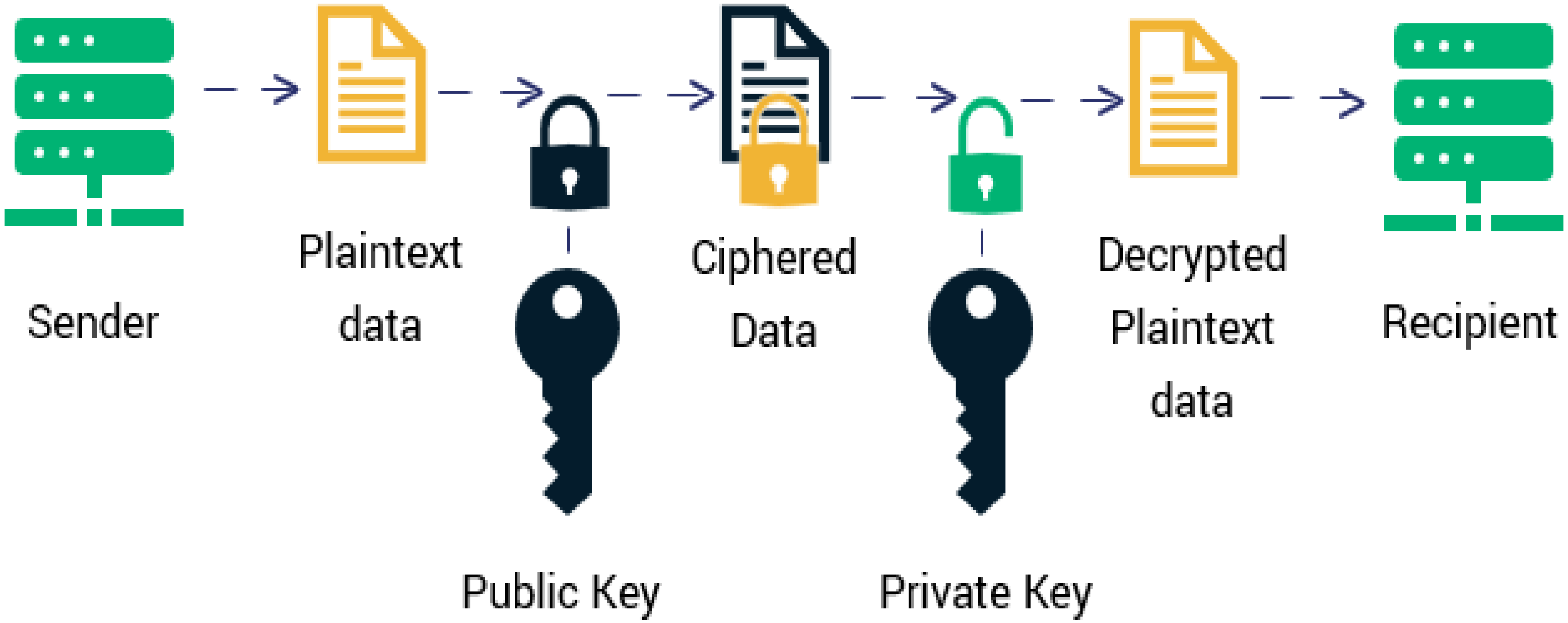
Validate Your Identity: The CA may request you to validate your identity before issuing the certificate. It could be in the form of email verification, sending official documents, or other means of authentication.

Download and install the certificate: If your identity can be verified, then a CA issues your certificate. Instructions will be provided about downloading/installing the certificate into your email client say, Outlook or Apple Mail.

Configuration of Your Email Client: Configure your email client to use the S/MIME certificate for encrypting and digitally signing all of your messages upon installation. Typically, this step is different for various clients. However, in general, you will need to pick the certificate within the security settings.

Test Your Setup: At a minimum, you will have to send an email to test that everything works fine with both encryption and digital signing.

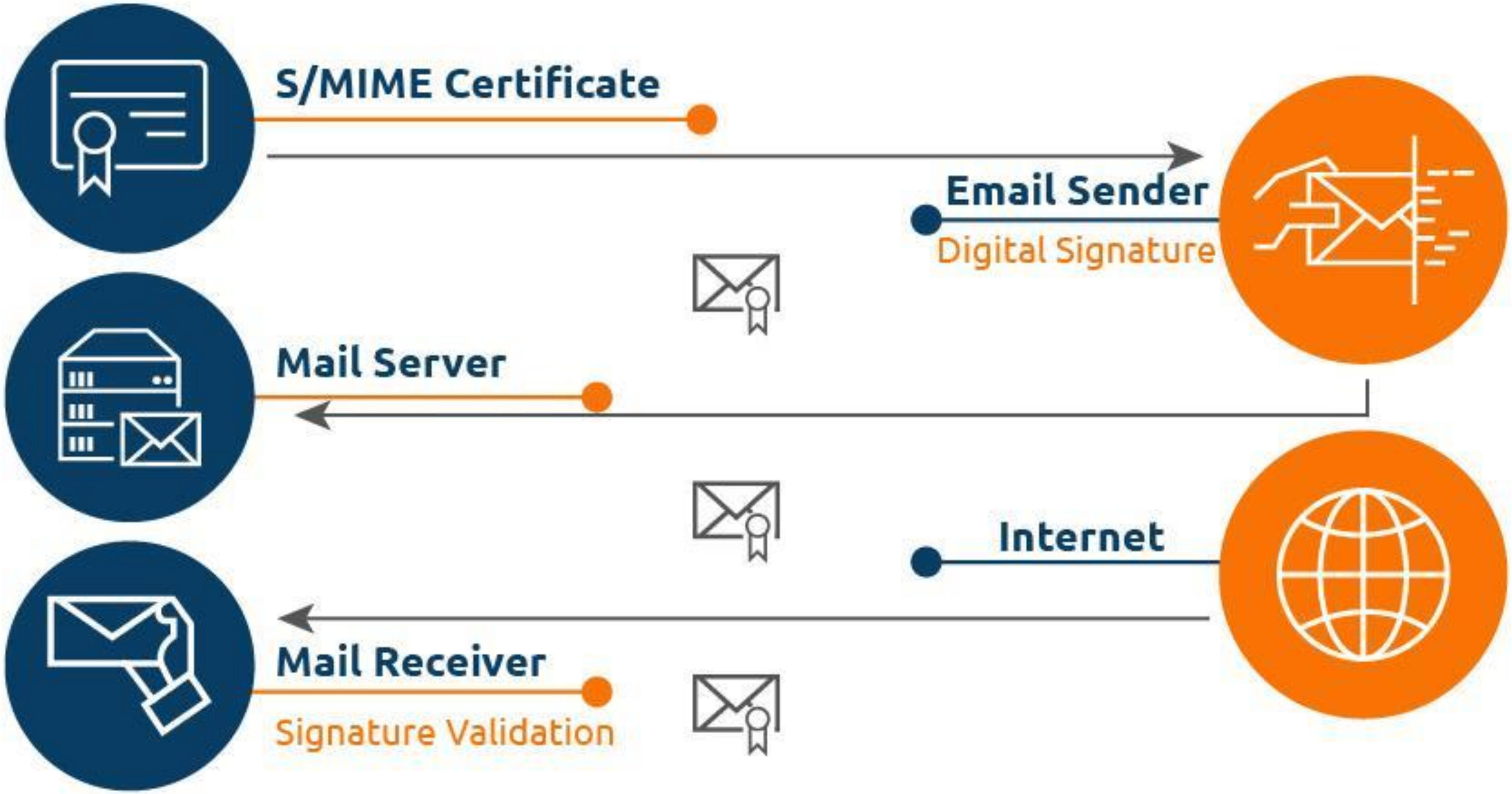
S/MIME CERTIFICATE



S/MIME CERTIFICATE

- **Sender:**
  - The sender prepares the plaintext data (email content).
- **Encryption with Public Key:**
  - The plaintext data is encrypted using the **public key** of the recipient.
  - This transforms the plaintext data into **ciphered (encrypted) data**, ensuring that only the intended recipient can read it.
- **Ciphered Data Transmission:**
  - The encrypted data is sent over the network to the recipient.
- **Decryption with Private Key:**
  - The recipient uses their **private key** to decrypt the ciphered data.
  - This transforms the ciphered data back into its original **plaintext** form.
- **Recipient:**
  - The recipient successfully receives and reads the decrypted plaintext data.

S/MIME certificate



S/MIME CERTIFICATE

S/MIME Certificate (Email Sender):

- The email sender uses an **S/MIME certificate** issued by a trusted Certificate Authority (CA).
- This certificate contains the sender’s **public key** and verifies the sender’s identity.
- The sender digitally signs the email using their **private key**, ensuring the email’s authenticity.

Mail Server:

The signed email is sent to the **mail server**, where it is processed and forwarded through the network.

The mail server does not alter the digital signature but ensures the email is routed to the correct recipient.

Internet Transmission:

The email travels through the **internet** securely, with the digital signature intact.

Anyone intercepting the email during transmission cannot modify or read its contents because:

> The email is encrypted using the recipient’s public key.
>
> The digital signature ensures tamper-proof communication.

Mail Receiver:

The recipient receives the email and uses their **private key** to:

> **Decrypt** the email contents.
>
> **Validate the digital signature** using the sender’s public key from their S/MIME certificate.

The signature validation ensures:

> The email is from the claimed sender (authentication).
>
> The email has not been altered during transmission (integrity).

Key Features of SMIME Certificate

- Industry-standard for public key encryption (asymmetric encryption) for MIME-based data.
- Offers two key email security functionalities — digital signatures and encryption.
- Digital signatures provide message integrity, authentication, and non-repudiation.
- Encryption provides data confidentiality (both for in-transit and at-rest data).

Because S/MIME uses asymmetric public key infrastructure (PKI), it employs two keys mathematically associated with each other to facilitates email security. By digitally signing your emails, the intended recipient can verify that the message was actually sent by you and hasn’t been tampered with or modified. When the email is en route from your computer to the recipient’s device, data encryption ensures that any attacker over the wire can’t read the contents of the message.

Any Query????

Thank you……