SMX2 MP07 SXA

# Serveis de xarxa

## UF02 – Correu electrònic i transmissió d'arxius

## Serveis de correu electrònic

Consisteix en l'enviament i recepció de missatges de text (a més d'un conjunt d'arxius adjunts) des d'un usuari origen a un destí de manera asíncrona (no cal que l'usuari destí estigui connectat).

## Altres funcions dels emails

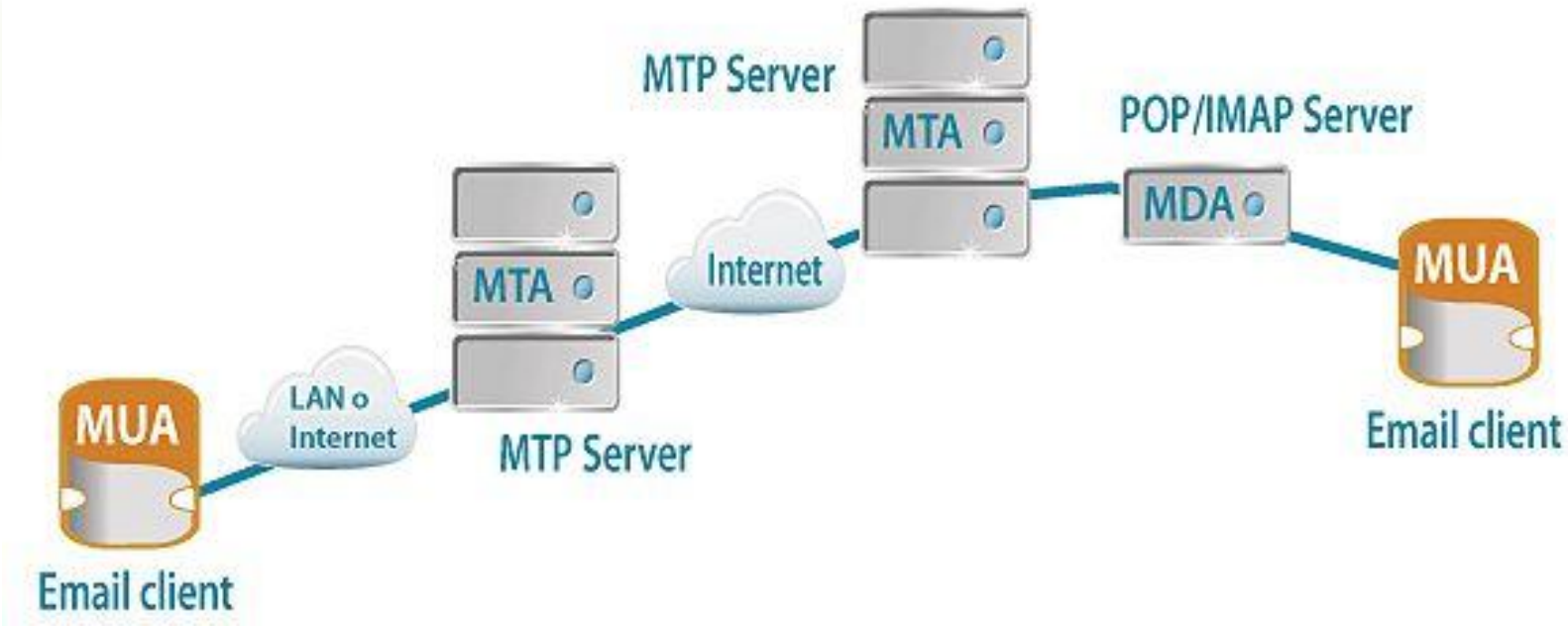
- És possible enviar un mateix missatge a un grup d'usuaris especificant diverses direccions o emprant llistes de correu.
- Existeixen mecanismes per informar a l'emissor si un missatge s'ha rebut correctament.
- Els missatges tenen una estructura interna ben definida.
- S'han facilitat interfícies d'usuari per facilitar l'enviament i recepció de correu.
- Els missatges poden incloure informació no textual, com imatges o sons.
- Els usuaris poden reenviar a altres usuaris els missatges que reben.
- És possible que els usuaris puguin consultar el correu des de qualsevol lloc i equip a través de bústies de correu.

## Agents involucrats

El sistema de gestió de correu electrònic es basa en la utilització de tres tipus d'agents:

- **MUA** (***Mail User Agent***): S'encarrega d'interaccionar amb els usuaris per enviar o rebre missatges. Tenen la forma de programes amb menús i opcions. Per exemple: Outlook, Thunderbird o Kmail de linux.
- **MTA** (***Mail Transfer Agent***): la seva tasca és la d'enviar els missatges des de l'origen fins al destí a través de la xarxa. Son serveis tipus 'dimonis' que executen els protocols d'enviament.
- **MDA** (***Mail Delivery Agent***): És el servidor de correu entrant.

# MUA, MTA i MDA


MTP Server
MTA
POP/IMAP Server
MDA
MTA
Internet
MUA
LAN o Internet
MUA
MTP Server
Email client
Email client

# Camps de les capçaleres (1/2)

Tots els missatges de correu electrònic consten de:

- **From (de)**: És l'adreça del creador del missatge.
- **To (para)**: És l'adreça o adreces dels que reben el missatge.
- **CC (en copia** o ***Carbon Copy*)**: Els destinataris que es posin aquí rebran còpia del correu.
- **BCC (en copia oculta** o ***Blind Carbon Copy*)** : Només els destinataris que hi figurin rebran una còpia del correu. Ningú més ho sabrà.

## Camps de les capçaleres

- **Sender** (*remitent*): És l'adreça de qui envia el missatge.
- **Date** (*data i hora*): Data i hora d'enviament del missatge.
- **Subject** (*assumpte*): És el títol del missatge. Quan l'usuari rebi el correu, és el que veurà del missatge per decidir si vol obrir-lo.
- **Reply-To** (*respondre a*): Nom d'usuari al qual cal enviar la resposta.
- **Message-Id** (*identificador*): Identificador del missatge.

## Camps del contingut

Els camps del contingut d'un missatge poden ser:

- ***Content-Description***: Descriu el contingut del missatge.
- ***Content-Id***: Identificador del contingut.
- ***Content-Transfer-Encoding***: Tipus de codificació del missatge (ASCII, base64, ...)
- ***Content-Type***: Tipus de contingut del missatge.

## Tipus de contingut del missatge

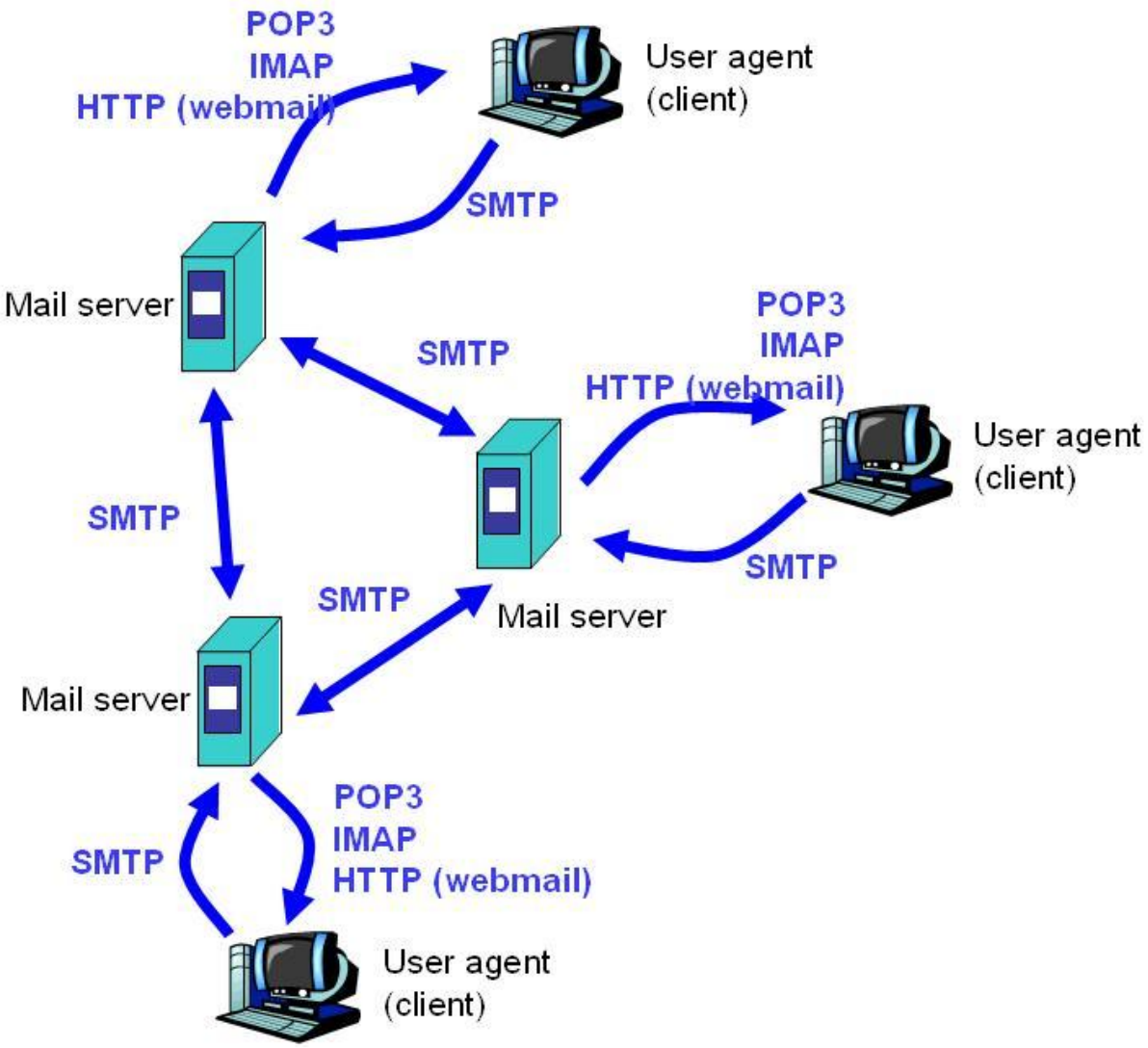
- Text/plain
- Text/richtext
- Text/rtf
- Image/gif
- Image/jpg
- Audio/basic
- Video/mpeg
- Application/javascript
- Application/pdf

## Transferència de correu

**SMTP**: Protocol senzill de transferència de correu (***Simple Mail TransferProtocol***)

- És el protocol encarregat d'**establir una connexió** entre l'origen i el destí, d'enviar les dades i desconnectar.
- Si es produeix un **error** durant la transmissió es genera un missatge de resposta a l'emissor indicant de possibles errors.
  - Comptes incorrectes
  - Bústies plenes
- És necessari que l'**emissor** i el **receptor** tinguin **sempre connexió a Internet** per a garantir la recepció dels paquets.
- El port emprat és el **25**.

# Protocol SMTP



## Lliurament dels correus als usuaris finals

- Els programes agents d'usuari (***outlook***, Mozilla Thunderbird, kmail, etc.) s'instal·len als equips client i es connecten a un servidor per descarregar el correu en els equips dels usuaris.

- Perquè els clients puguin establir una connexió sobre el servidor de correu s'utilitzen protocols com POP3 (***Post Office Protocol***) o *IMAP* (***Internet Message Access Protocol***).

## Protocols POP3 i IMAP

- ***POP3*** (***post office protocol*** o **protocol d'oficina de correus**)
  - És el protocol que permet rebre correus electrònics des del servidor.

- ***IMAP*** (***Internet message access protocol*** o **protocol d'accés a missatges d'Internet**)
  - És un protocol que permet veure correus electrònics des del servidor, però no baixa cap informació a la nostra màquina.

# Diferències entre POP3 i IMAP

| POP | WEB |
| --- | --- |
| Es pot veure el correu sense estar connectat a Internet si prèviament s'ha baixat a l'ordinador. | Només es poden veure els correus quan s'està connectant a Internet, ja que sempre són en el servidor. |
| Els arxius adjunts s'obren més de pressa, perquè es desen al nostre equip amb els correus. | Els arxius adjunts no es descarreguen (si no volem) a la nostra màquina, la qual cosa evita possibles infeccions. |
| El límit d'arxius és el del vostre disc dur, ja que els correus s'esborren del servidor un cop baixats (tret que s'especifiqui el contrari). | La limitació depèn del servidor de correu. |
| En cas d'haver-hi un problema amb el nostre ordinador, perdríem tots els correus. | Es fan còpies de seguretat periòdiques, i la possibilitat de perdre correus és molt petita. |
| Funciona sobre el port 110. | Funciona sobre el port 143 |

## Seguretat i privacitat

Hi ha problemes de seguretat i privacitat en els missatges de correu per 3 raons fonamentals:

1. Els missatges circulen lliurement per la xarxa des d'un origen cap a un destí i **poden ser interceptats** pel seu camí.

2. Els protocols de transferència de correu envien missatges **sense xifrar**.

3. El nom d'origen **pot ser manipulat**, de forma que no es pot comprovar la identificació de la persona que envia el missatge.

## Problemes de seguretat

Els problemes de seguretat dels emails més comuns són:

- **Virus** d'email.
- ***Spam***: correu electrònic comercial no sol·licitat.
- ***Phishing***: intenten aconseguir informació bancària.
- Falsejament d'identitat (***E-mail spoofing***): la informació de capçalera es canvia per fer veure que el missatge procedeix d'una font coneguda.
- Bombardeig de correu (***E-mail bomb***): És l'enviament intencionat de volums grans de missatges a una adreça objectiu. (atac ***DOS***)
- Altres problemes de seguretat.

## Programes per la seguretat i privacitat

El concepte clau per a la confiança en les comunicacions per correu electrònic és la **signatura digital**, que permet **assegurar** que un **emissor** és qui diu ser i garanteix també que el **contingut del missatge** no s'ha alterat per tercers. Per implementar la **signatura digital** i el **xifratge** cal utilitzar **certificats digitals**.

## Programes per la seguretat i privacitat

- L'***MTA*** (***Mail Transfer Agent***) i els servidors de correus transporten missatges independentment del fet que estiguin xifrats o signats.
- Són **els clients de correu** els que han de proporcionar a l'usuari la **capacitat de xifrar** i **signar missatges**.

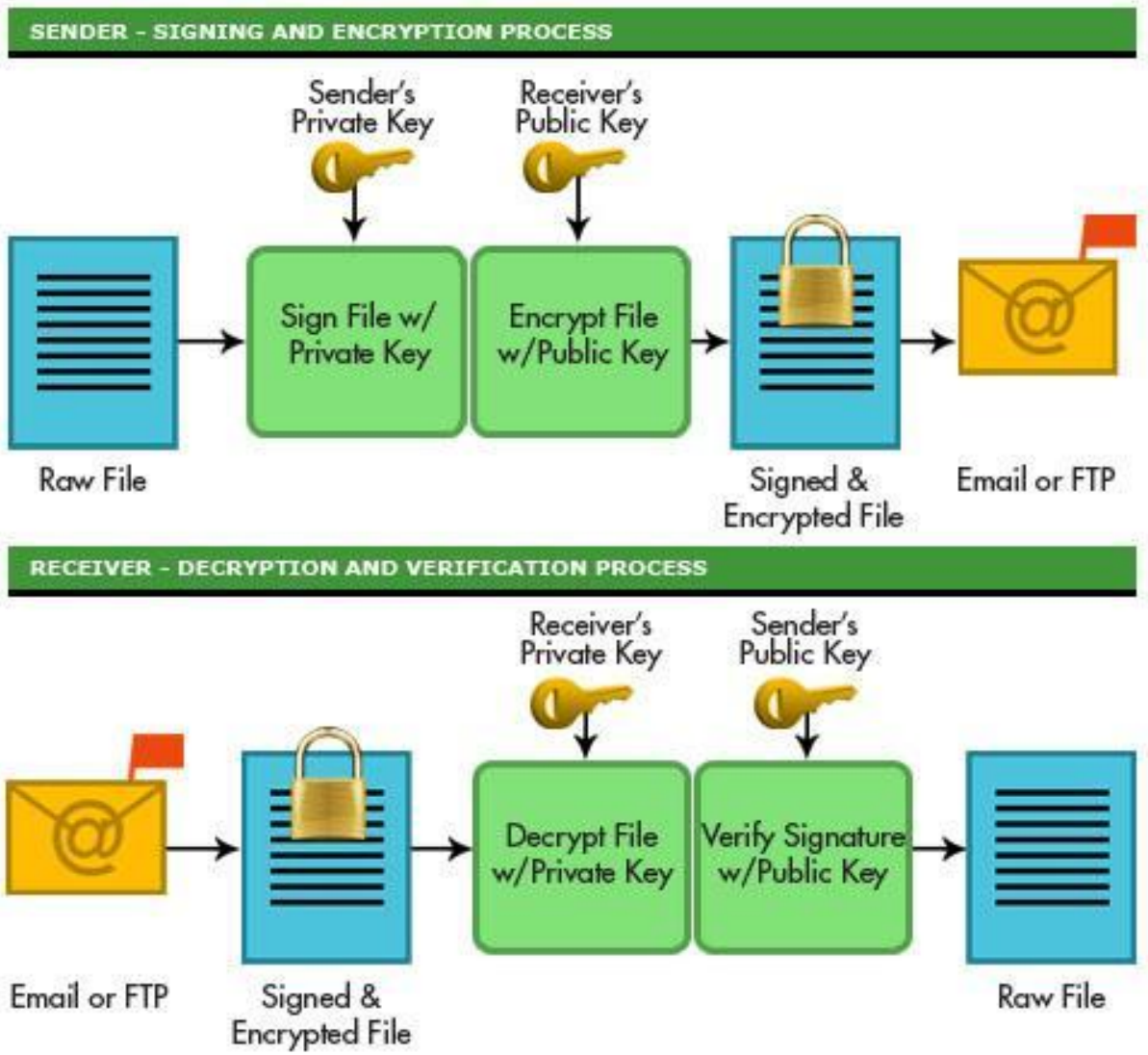
## Programes per la seguretat i privacitat

Un dels programes més emprats és ***PGP*** (*Pretty Good Privacy*).

***PGP*** envia el missatge xifrat juntament amb la clau de sessió també xifrada.

L'operació de xifratge es fa mitjançant una **clau pública** subministrada pel **receptor**, mentre que el **desxifrat** d'aquesta clau es fa amb una **clau privada** que solament coneix el **receptor**.

# PGP


SENDER - SIGNING AND ENCRYPTION PROCESS
Sender's Private Key
Receiver's Public Key
Sign File w/ Private Key
Encrypt File w/Public Key
Raw File
Signed & Encrypted File
Email or FTP
RECEIVER - DECRYPTION AND VERIFICATION PROCESS
Receiver's Private Key
Sender's Public Key
Decrypt File w/Private Key
Verify Signature w/Public Key
Email or FTP
Signed & Encrypted File
Raw File