

# Seguridad en Redes

## Práctica 3.2. E-mail seguro

### Preparación del entorno

En esta práctica usaremos tres MVs: `servidor`, `host1` y `host2`. La MV `servidor` actuará como servidor de correo saliente (smtp) y entrante (imap). Las MVs `host1` y `host2` actuarán como clientes de correo.

Cada MV tendrá dos interfaces de red:

- El adaptador 1 (`eth0`) configurado en modo NAT para instalar los paquetes necesarios (una vez instalados los paquetes necesarios y configuradas las MVs, se deshabilitará la interfaz `eth0` para cualquier tipo de conflicto.)
- El adaptador 2 (`eth1`) configurado en modo red interna, que se usará comunicarnos entre las distintas máquinas virtuales. Las tres interfaces `eth1` deben estar conectados a la misma red interna (por ejemplo, la llamamos `net1`)

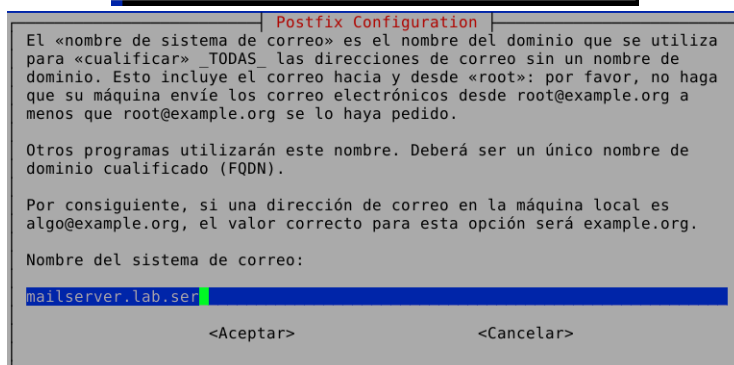
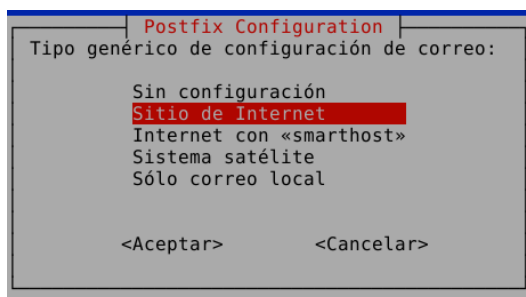
### Configuración de servidor

En el servidor instalaremos telnet, SSH, el servidor de transferencia de correo SMTP (`postfix`) y el servidor de correo entrante IMAP (`dovecot`):

```
$ sudo apt-get update
$ sudo apt-get install telnet telnetd ssh
$ sudo apt-get install postfix
```

Al instalar `postfix`, aparecerán dos ventanas de configuración:

- En tipo genérico de configuración seleccionar "Sitio de Internet"
- En nombre del sistema de correo introducir "mailserver.lab.ser"



```
$ sudo apt-get install dovecot-core dovecot-imapd
```

A continuación configuramos el nombre de host del sistema (/etc/hostname), el archivo de nombres de hosts (/etc/hosts) y el archivo de configuración de red (/etc/network/interfaces) para establecer una configuración estática

Edita /etc/hostname y sustituye su contenido por el siguiente:

```
mailserver.lab.ser
```

Edita /etc/hosts y añade al final las siguientes líneas:

```
192.168.1.1    mailserver.lab.ser
192.168.1.2    host1.lab.ser
192.168.1.3    host2.lab.ser
```

Edita /etc/network/interfaces y añade al final las siguientes líneas:

```
auto eth1
iface eth1 inet static
    address 192.168.1.1
    netmask 255.255.255.0
```

El siguiente paso es dar de alta dos cuentas de usuario en el sistema, que estarán asociados a las cuentas de correo electrónico:

```
$ sudo adduser ana
(Nombre real: Ana Gil Molina,
Elegir una contraseña fácil de recordar)
```

```
$ sudo adduser benito
(Nombre real: Benito Torres Rubio,
Elegir una contraseña fácil de recordar)
```

Finalmente reinicia el servidor:

```
$ sudo init 6
```

Cuando arranque desactiva la interfaz eth0:

```
$ sudo ifdown eth0
```

### Configuración de host1

En los PCs de los clientes instalaremos SSH y el cliente de correo electrónico (icedove):

```
$ sudo apt-get update
$ sudo apt-get install ssh
$ sudo apt-get install icedove
```

A continuación configuramos el nombre de host del sistema (/etc/hostname), el archivo de nombres de hosts (/etc/hosts) y el archivo de configuración de red

(/etc/network/interfaces) para establecer una configuración estática

**Edita /etc/hostname y sustituye su contenido por el siguiente:**

```
host1.lab.ser
```

**Edita /etc/hosts y añade al final las siguientes líneas:**

```
192.168.1.1    mailserver.lab.ser
192.168.1.2    host1.lab.ser
192.168.1.3    host2.lab.ser
```

**Edita /etc/network/interfaces y añade al final las siguientes líneas:**

```
auto eth1
iface eth1 inet static
    address 192.168.1.2
    netmask 255.255.255.0
```

**Finalmente reinicia host1:**

```
$ sudo init 6
```

**Cuando arranque desactiva la interfaz eth0:**

```
$ sudo ifdown eth0
```

## **Configuración de host2**

**En los PCs de los clientes instalaremos SSH y el cliente de correo electrónico (icedove):**

```
$ sudo apt-get update
$ sudo apt-get install ssh
$ sudo apt-get install icedove
```

**A continuación configuramos el nombre de host del sistema (/etc/hostname), el archivo de nombres de hosts (/etc/hosts) y el archivo de configuración de red (/etc/network/interfaces) para establecer una configuración estática**

**Edita /etc/hostname y sustituye su contenido por el siguiente:**

```
host2.lab.ser
```

**Edita /etc/hosts y añade al final las siguientes líneas:**

```
192.168.1.1    mailserver.lab.ser
192.168.1.2    host1.lab.ser
192.168.1.3    host2.lab.ser
```

**Edita /etc/network/interfaces y añade al final las siguientes líneas:**

```
auto eth1
iface eth1 inet static
    address 192.168.1.3
    netmask 255.255.255.0
```

**Finalmente reinicia host2:**

```
$ sudo init 6
```

Cuando arranque desactiva la interfaz eth0:

```
$ sudo ifdown eth0
```

## Configuración de SMTP e IMAP sin seguridad TLS

### Configuración de postfix (protocolo SMTP)

El protocolo de transferencia de correo SMTP está implementado en el `servidor` a través del servicio `postfix`. Para configurar SMTP sin seguridad TLS, edita el archivo configuración `/etc/postfix/main.cf` y modifica las siguientes líneas

```
...
smtpd_use_tls=no
...
mynetworks = 127.0.0.0/8, 192.168.1.0/24
```

A continuación, reinicia el servicio `postfix`:

```
# service postfix restart
```

Comprueba mediante `netstat -ant` que se abre únicamente el puerto 25, correspondiente a SMTP sin seguridad TLS (los puertos 465 y 587 correspondientes a SMTP con seguridad TLS deben estar cerrados)

Para comprobar que el servidor SMTP funciona, conéctate al puerto 25 del `servidor` ejecutando el siguiente comando en el propio `servidor`:

```
telnet localhost 25
```

A continuación introduce el comando `HELO mailserver.lab.ser` y cierra la conexión con el comando `QUIT`.

**Entrega #1:** Copia y entrega todos los mensajes intercambiados con el servidor SMTP en esta comunicación

### Configuración de dovecot (protocolo IMAP)

El protocolo de correo entrante IMAP está implementado en el `servidor` a través del servicio `dovecot`. Para configurar IMAP sin seguridad TLS, hay que editar y modificar los siguientes archivos de configuración:

- Edita `/etc/dovecot/dovecot.conf` y modifica la siguiente línea para habilitar IMAP en todas las interfaces de red:  

```
listen = *, ::
```
- Edita `/etc/dovecot/conf.d/10-ssl.conf` y modifica la siguiente línea para configurar IMAP sin seguridad TLS:  

```
ssl = no
```

- Edita `/etc/dovecot/conf.d/10-auth.conf` y modifica la siguiente línea para permitir la autenticación del cliente en texto plano (sin cifrado):  
`disable_plaintext_auth = no`

A continuación, reinicia el servicio `dovecot`:

```
# service dovecot restart
```

Comprueba mediante `netstat -ant` que se abre únicamente el puerto 143, correspondiente a IMAP sin seguridad TLS (el puerto 993 correspondiente a IMAP con seguridad TLS debe estar cerrado)

Para comprobar que el servidor IMAP funciona, conectate al puerto 143 del servidor ejecutando el siguiente comando en el propio servidor:

```
telnet localhost 143
```

A continuación introduce los siguientes comandos:

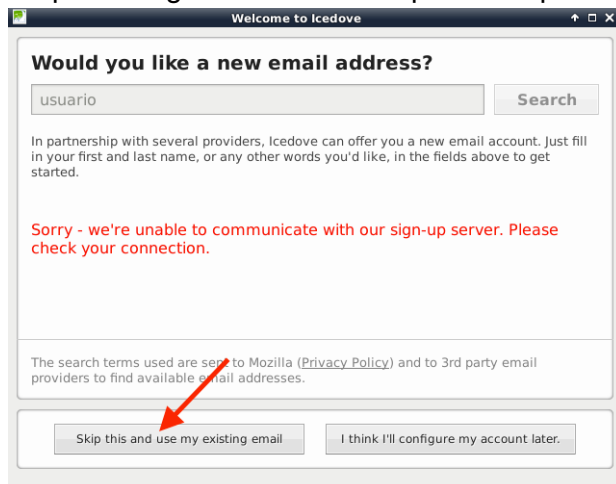
```
a LOGIN [username] [password]
(para hacer login con un usuario, p. ej. benito y su correspondiente contraseña)
a LIST "" *
(para listar los buzones de correo del usuario, p. ej. Inbox, Sent, Trash)
a EXAMINE Trash
(para examinar el buzón de papelera Trash)
a LOGOUT
(para salir de la sesión)
```

**Entrega #2:** Copia y entrega todos los mensajes intercambiados con el servidor IMAP en la comunicación anterior

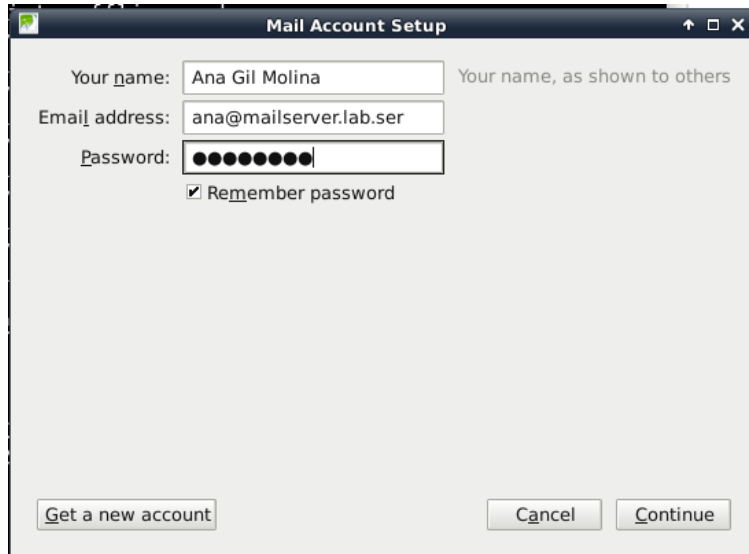
## Configuración la aplicación cliente icedove

Arranca en `host1` el cliente de correo `icedove` y configura la cuenta de correo `ana@mailserver.lab.ser`

En primer lugar selecciona la opción “Skip this and user my existing email”



A continuación introduce los datos de usuario y contraseña del usuario `ana` creado en el servidor de correo:



Pulsa el botón “Continue” y aparecerá una última ventana de “Warning!” indicando que el servidor no utiliza cifrado ni para correo entrante ni para correo saliente. Pulsa el botón “Done” para terminar



Repite las acciones anteriores en la máquina `host2` con cuenta de correo `benito@mailserver.lab.ser` para el usuario `benito`.

### Entrega #3:

- Envía un correo electrónico de Ana a Benito y captura todo el tráfico (SMTP e IMAP) ejecutando `wireshark` en el servidor.
- En `wireshark`, elige un paquete SMTP de la comunicación anterior. Usa la opción “Analyze → Follow TCP stream” para visualizar toda la conversación entre cliente y servidor SMTP en formato ASCII. Copia y entrega dicha conversación.
- Repite la misma operación para visualizar la conversación entre el cliente y el servidor IMAP en formato ASCII. Copia y entrega dicha conversación.


## Seguridad SMIME extremo a extremo (cliente de correo)

A continuación vamos a implementar seguridad extremo a extremo mediante SMIME, creando e instalando un certificado digital para cada usuario, que nos permita intercambiar correo electrónico cifrado y/o firmado entre ambos usuarios.

Para ello, en primer lugar es necesario crear una autoridad de certificación (`demoCA`) con autofirma y después crear un certificado digital para cada usuario, que será firmado por dicha CA, todo ello siguiendo las instrucciones de la práctica 2.3. Estas operaciones, que realizaremos en el `servidor`, son las siguientes:

1. Crea una autoridad de certificación (`demoCA`) con autofirma
2. Crea dos solicitudes de firma de certificado (CSR) para Ana Gil Molina y para Benito Torres Rubio (IMPORTANTE: introducir, cuando se pida, sus correspondientes cuentas de correo: `ana@mailserver.lab.ser` y `benito@mailserver.lab.ser`). Los archivos de clave privada y CSR de cada usuario serán los siguientes:
  - o Usuario Ana: `ana_key.pem`, `ana_csr.pem`
  - o Usuario Benito: `benito_key.pem`, `benito_csr.pem`
3. Firma las dos solicitudes de certificado anteriores
  - o Genera dos certificados: `ana_cert.pem` y `benito_cert.pem`
4. Exporta certificados a formato PKCS12
  - o Genera los archivos `ana_cert.p12` y `benito_cert.p12` (estos ficheros almacenan el certificado junto con la clave privada)
5. Copia los siguientes ficheros a `host1` (podemos usar el comando `scp [file] usuario@host1.lab.ser:.`)
  - o `ana_cert.p12` (certificado y clave privada de Ana)
  - o `benito_cert.pem` (certificado de Benito)
  - o `demoCA/cacert.pem` (certificado de la CA)
6. Copia los siguientes ficheros a `host2` (podemos usar el comando `scp [file] usuario@host2.lab.ser:.`)
  - o `benito_cert.p12` (certificado y clave privada de Benito)
  - o `ana_cert.pem` (certificado de Ana)
  - o `demoCA/cacert.pem` (certificado de la CA)

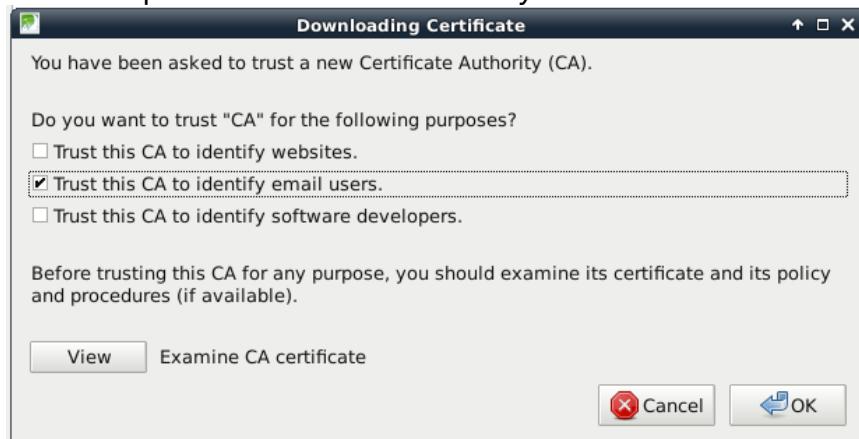
A continuación, es necesario instalar los certificados en los cliente de correo electrónico (`icedove`) de cada uno de los usuarios. En `host1`, ir a propiedades de la cuenta de correo (`account settings`) de la cuenta de correo `ana@mailserver.lab.ser` y realizar las acciones que se indican:

- Selecciona Menú () → *Preferences* → *Account Settings* → *Security*. Se mostrará la siguiente ventana con tres secciones (*Digital signing*, *Encryption* y *Certificates*)



- En la sección *Certificates* pulsa *View certificates* e importa los siguientes certificados:

- Pestaña *Autorities*: importa `cacert.crt`  
Marca la opción “*Trust this CA to identify email users*”



- Pestaña *Your certificates*: importa `ana_cert.p12`
- Pestaña *People*: importa `benito_cert.pem`
- Sección *Digital Signing*
  - Selecciona e importa el certificado de Ana
  - Marca Opción “*Digitally sign messages*” (esta opción firmará todos los mensajes enviados)
- Sección *Encryption*
  - Selecciona e importa el certificado de Ana (posiblemente esté ya importado, ya que la operación anterior elige, por defecto, el mismo certificado para cifrado y para firma)
  - Marca Opción “*Required*” (esta opción cifrará todos los mensajes enviados)



Repite las mismas operaciones en `host2`, cambiando lo siguiente al importar los certificados:

- En la sección *Your certificates*: importa el certificado `benito_cert.p12`
- En la sección *People*: importa el certificado `ana_cert.pem`.

Comprueba que cuando se envía un correo de Ana a Benito (o viceversa), éste se envía cifrado y encriptado. Esto puede verse en el propio mensaje de correo (enviado o recibido), que incluye estos dos símbolos:

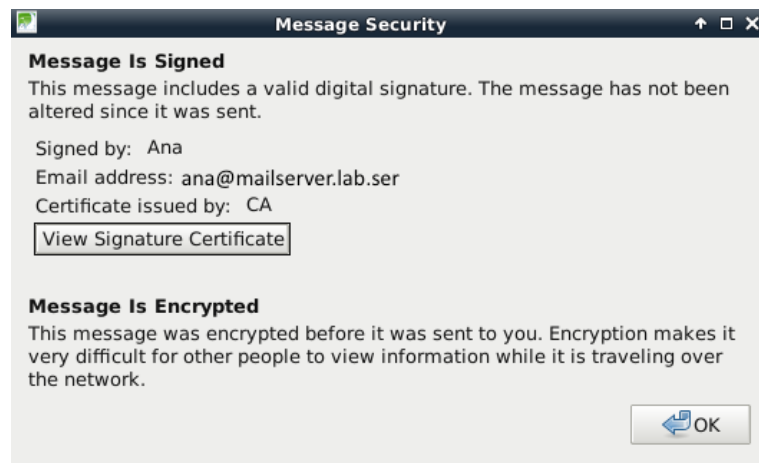


(correo firmado)

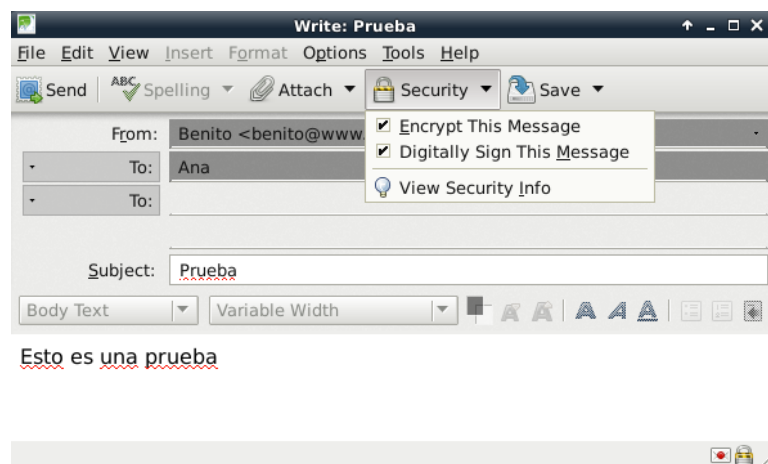


(correo cifrado)

Pulsando sobre cualquiera de estos dos símbolos aparecerá la siguiente ventana, donde se puede verificar la firma:



Con la configuración seleccionada, se firmarán y cifrarán por defecto todos los mensajes enviados. No obstante, cuando se compone un mensaje, podemos elegir si lo queremos cifrar y/o firmar, mediante la opción *Security* en la propia ventana del mensaje:



**Entrega #4:**

- Envía un correo electrónico de Ana a Benito firmado y cifrado. Captura todo el tráfico (SMTP e IMAP) ejecutando `wireshark` en el `servidor`.
- En `wireshark`, elige un paquete SMTP de la comunicación anterior. Usa la opción “*Analyze → Follow TCP stream*” para visualizar toda la conversación entre cliente y servidor SMTP en formato ASCII. Copia y entrega dicha conversación.
- Repite la misma operación para visualizar la conversación entre el cliente y el servidor IMAP en formato ASCII. Copia y entrega dicha conversación.

**Entrega #5:** Compara la conversación entre el cliente y el servidor SMTP de la entrega 3 y de la entrega 4. Busca en ambos casos el campo `Content-Type`. Cópialos y pégalos y explica brevemente qué significa dicho campo en uno y otro caso.