

# Práctica 3 Seguridad en Redes y Servicios

Raúl Calderón Moya

## El protocolo TLS

Pregunta 1. Dibuja un diagrama de intercambio de mensajes que muestre el procedimiento de establecimiento de sesión que lleva a cabo TLS. Incluye en el diagrama las claves de cada una de las entidades involucradas, así como todo el material criptográfico intermedio.

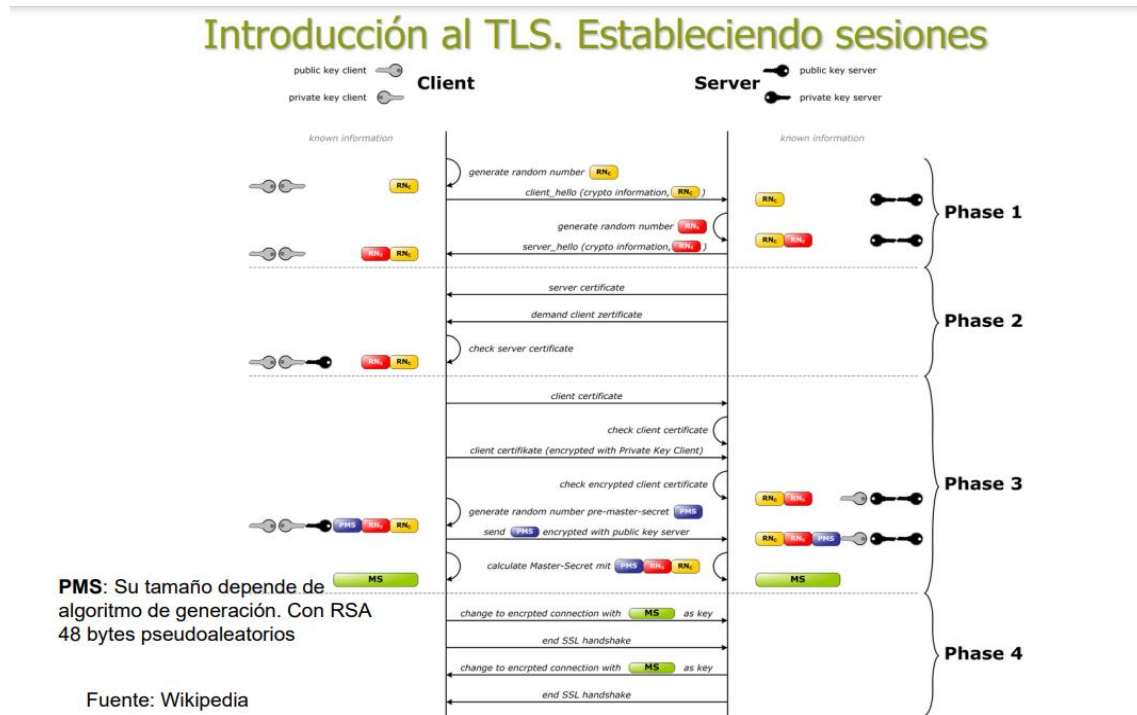


Ilustración 1 Establecimiento sesiones TLS

## Protocolo Handshake con autenticación cliente mediante certificados

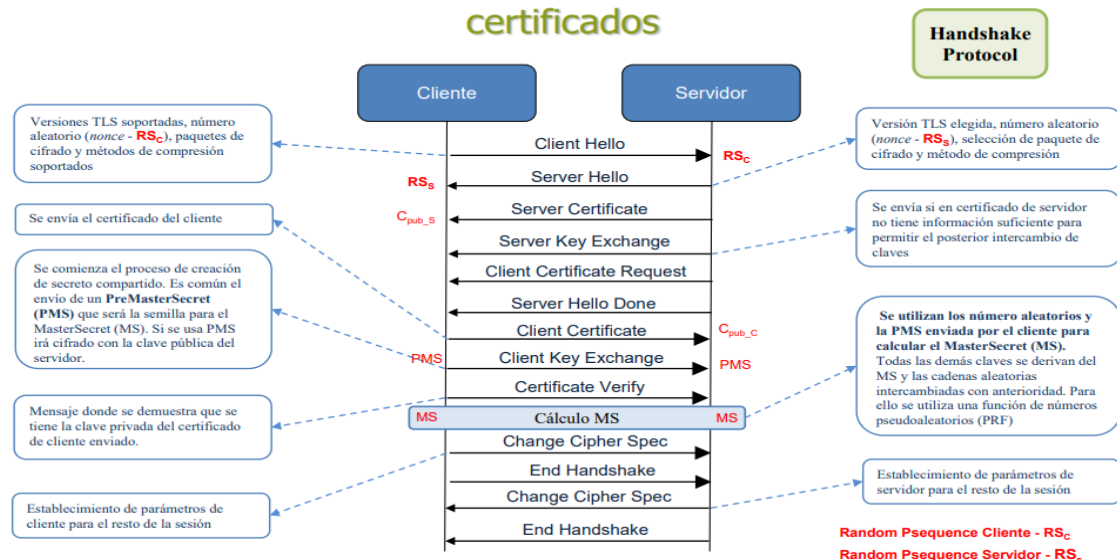


Ilustración 2 Protocolo Handshake

### Pregunta 2. ¿Qué diferencia existe entre el protocolo TLS y el SSL?

SSL es un protocolo criptográfico para garantizar comunicaciones seguras en red. El protocolo SSL debe ofrecer integridad, confidencialidad y autenticación en una red entre un cliente y un servidor.

Tanto SSL como TLS son protocolos utilizados para la autenticación entre entidades como paso previo al intercambio de las claves criptográficas.

Ambos deben acordar una serie de parámetros antes de establecer la comunicación y así poder llevar a cabo de manera segura la comunicación entre el navegador web y el servidor. Un ejemplo puede ser los algoritmos criptográficos que se utilizan para cifrar, intercambiar claves y para realizar la firma como RSA, DES, AES, entre otros. Después de esto, se debe realizar el intercambio de claves y la autenticación para dar lugar al intercambio de tráfico entre ambas partes.

La diferencia entre SSL y TLS es que TLS es una versión posterior a SSL con ciertas mejoras respecto a SSL relacionadas con aspectos de seguridad. TLS ofrece protección frente a nuevos ataques, proporcionar nuevos algoritmos criptográficos y evitar que se pueda forzar a usar versiones del protocolo más vulnerables, entre otros.

### Pregunta 3. ¿Se puede utilizar TLS sobre un nivel de transporte UDP?

Sí, existe el protocolo DTLS, el cual es TLS sobre UDP.

# TLS para comunicaciones web

Pregunta 4. Dibuja la pila de protocolos definida para una aplicación que se base en HTTPS.

|                            |
|----------------------------|
| HTTPS (Capa de Aplicación) |
| SSL o TLS                  |
| TCP (Capa de Transporte)   |
| IP (Capa de Red)           |

Pregunta 5. Busca servicios que permitan la conexión mediante HTTPS. ¿Qué ocurre en un navegador web (Firefox, Chrome, etc.) cuando realiza una conexión satisfactoria con un servidor de este tipo? ¿Cómo avisa a al usuario?

Los servicios que hacen uso de HTTPS para conexiones son aquellos que utilizan SSL/TLS consiguiendo establecer una comunicación segura entre cliente (navegador web) y servidor.

Para avisar al usuario lo que hace el navegador es representar mediante un candado que la conexión es segura. Se muestra una figura de ejemplo:

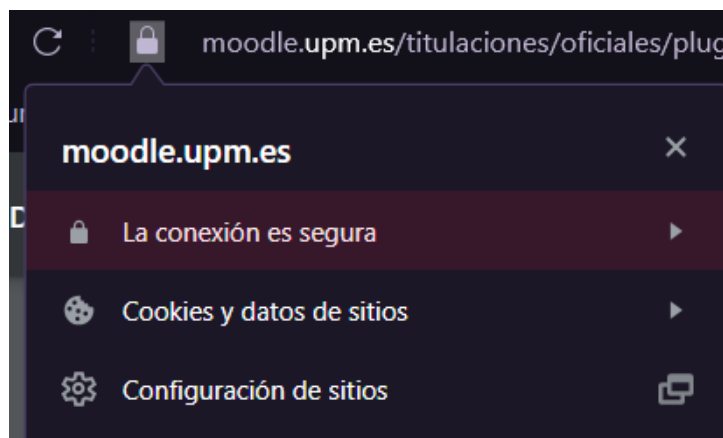


Ilustración 3 Captura protección HTTPS en navegador OperaGX

Pregunta 6. ¿Cómo puede realizar un servidor web una autenticación fuerte mediante el protocolo HTTPS? La autenticación fuerte descarta el uso de nombre de usuario y contraseña como único método de autenticación para realizar el control de acceso. Pon un ejemplo en el que la Escuela implementase un mecanismo de autenticación criptográficamente fuerte para todo el personal. ¿Qué elementos, además del servidor web y los navegadores, serían necesarios?

Para poder realizar una autenticación fuerte mediante el protocolo HTTPS, el servidor puede solicitar al usuario una huella digital o token de seguridad junto con usuario y contraseña. La autenticación tiene como objetivo asegurar que la persona que se identifica es realmente quién dice ser.

Un ejemplo, de la escuela sería el uso de un sistema de huella que junto con el nombre de usuario y contraseña se pudiera autenticar garantizando que la entidad es justamente el alumno que dice ser y no se está haciendo pasar por él otra entidad. Otro ejemplo podría ser la autenticación de doble factor en una página web como puede ser Moodle de la UPM.

**Pregunta 7. ¿Es el protocolo TLS aplicable a otros protocolos además del HTTP? Pon al menos dos ejemplos reales.**

Sí, el protocolo TLS se puede utilizar en FTP y SMTP. Para SMTP sería correo electrónico y para FTP se emplearía para transferencia de archivos.

## TLS/SSL en detalle

### 1. Generación de claves criptográficas

**Pregunta 8. Analiza brevemente los distintos comandos que tiene OpenSSL invocando el comando: `man openssl`**

OpenSSL es una herramienta de cifrado que implementa los protocolos SSL y TLS y los estándares de cifrado que requieren dichos protocolos.

Los comandos que tiene OpenSSL para la realización de esta práctica se pueden consultar ejecutando el comando “`man openssl`” y algunos de los más importantes son los siguientes:

- `genrsa`: Generación de la clave privada RSA.
- `req`: Gestión de solicitud de firma de certificado X.509 en formato PKCS#10.
- `rsa`: Gestión de clave RSA.
- `s_client`: Sirve para implementar un cliente SSL/TLS genérico que pueda establecer una conexión transparente con un servidor remoto a través SSL/TLS. Está destinado a fines de prueba y solo proporciona una funcionalidad de interfaz rudimentaria, pero internamente utiliza principalmente toda la funcionalidad de la biblioteca SSL de OpenSSL.
- `s_server`: Esto implementa un servidor SSL/TLS genérico que acepta la conexión de un cliente remoto que habla SSL/TLS. Está destinado a fines de prueba y solo proporciona una funcionalidad de interfaz rudimentaria. Proporciona un protocolo propio orientado a la línea de comandos para probar las funciones de SSL y una función de respuesta HTTP simple para emular un servidor web compatible con SSL/TLS.
- `x509`: Gestión de datos del certificado X.509.

## Captura de man openssl



Ilustración 4 Ejecución de man openssl

Pregunta 9. Genera un par de claves RSA de tamaño 4096 bits mediante OpenSSL. ¿Dónde se almacenan esas claves? ¿Cuál es el exponente de la clave pública?

Los comandos utilizados para crear las claves son:

```
user@user-virtual-machine:~$ openssl genrsa -out clave_privada.pem 4096
user@user-virtual-machine:~$ openssl rsa -in clave_privada.pem -pubout -out clave_publica.pem
writing RSA key
```

Ilustración 5 Generación de clave secreta y pública.

Las claves se almacenan en los ficheros clave\_privada.pem y clave\_publica.pem para almacenar la clave privada y la clave pública respectivamente. La clave pública como se puede apreciar se genera a partir de la clave privada.

En cuanto a ubicación de los archivos clave\_privada.pem y clave\_publica.pem en este caso al estar en user, se almacenarán en el usuario root.

Se muestran las claves generadas:

```
user@user-virtual-machine:~$ cat clave_privada.pem
-----BEGIN PRIVATE KEY-----
MIIEJRAIBADANBgkqhkiG9w0BAQEFAAQCCS4wggkqAgEAAoICAQDg0LwLXBuVlyuR
RLBpa/2spFlaTo10n0YJIqNgC/zapLmA07FMDzqxk+PsvWIS1eAFEBILx6Hk+qfs
lj2VNsRQoxuG4QrlehnTTwydk6v5U/w6basW03Xq/XRESLIudugK0sW3fU86eps6
k/e5Qj76TNLXC6bu1Pu1e2KLWRAFP87tsdJw0cm4kY+TnwRVYU4Q1JWF3VZ3RLm
nJ1uSU591dhw53CfB+53NRwB3y0FXX0FFfbvyczLzb7BUhN7nu67LD8trwzLJULVh1
KL3Ew424g1gK6sFmWd50/bmk8au0DuArYxUbCtBhKCB7JSLNztWz985/xpeVoyrL
lrvsu8a6gqkLGSQ+XrTyJYW10qMpZwttFAgR05JcyTqjYgZ8BMKx60eZhzEzY4lSk
YU3vvtUJVXWBJNG15lMHbHeUpkULsL5zjK9d7ddAs8xBX4MBD8nQNKv2zCyBCFQ
BgQ93lWF570E3CaSfcJdTnHYAD8L31ANS1DJKUI705GjInBI4EFT2VN6NHJBVCZF
z/N3qcxU9/G8pqxyVdb0PW8rBhoxTFmpZyZpxNxtYhvaYq4oFautAZCz0dMzXgXJ
qPaRKn9FFCjRfKkmW89P0PkgL+9PbJz0h+9PbJz0h+9PbJz0h+9PbJz0h+9PbJz0h
BxwEDlYald7FATy8U7H0MswATAOI+WIIDAQABAQICABBIQODZCv2a3jQKYN8+tjVH+
apcX2WQ4ZPovEruDS20Klo+eGtLHa+N26ACArqumSsaJ6z/fdexpTVP4fTFVxEk
FH4UjPvDWAyR04LA3lkmIwLEnX+pu9X+ms0sv4UmL5KGcyUN/Tm0Z58hLcVdPEfP
XFX1V2yKQIYVvHutNGxFGQyvwGB5Zq2CMSPzTejjBnhsVsnpyQtugk/qFPzykVHE
spkMLFBnQDFfcgFZ5lXN2e0Tz3VhUc85P3kzGrm97dSud015Ve3Fva0dI/brsXIK
C/ZZH74qA3CCHU+LXAKj50m99JQlf500otB1gE9E5Kqgg5ZNYLKEPjXE5pI3Jub
k2M4d+x7T1HYSLHohRBCITrF3Fm9vqxNwrn0LyZkxp9PCAAX1cRbX1ghJvQPIYr
Zc6tUYG00OcXmsNYWphnOoJptv8RyE51exBAgThx4D7Kvz04WvDjxd9lLeVZk+UL
bMdFu5dwEx0wJaaVf64TecX5BZ5ew4850fKxNN+5X0rz5nsFvtZJQnLYNmG9C9GuL
oRlhbQ12tgyAylVuaC1Q3ZVMnHcYV6TpxBEjSBQE9s0uYxrReQr/FZbfaA23j6v0
r/BFXa4bFVG+hgSMJohAVgguCvm4BYwA8Qjn5BFW8J41Lx4ZAwLytlEANbvdd60ku
Q7u01uH3ALuR3/FIXc8A0IBA0D2eHoLwIwKs/RCAxJA1e8grCvqXfFpE9Rk05QA+
8AAP/SeSk/Iw5307H4ba6nsn4XEckVAwqgmJjKJ8JaoUfVeSk5FhmdumnmhLVEtB
VvBRKf8r+NBN0y3jEhyKczbvXuj2QCq+VtXMI90R7eKFLNjIa09/sXxvgo1dogVW
wKcBsy8oqLiEtVdyXZz+xZlKrhJEMBqn1EBz8qGzjnFNVp75Pkmx/70NRZjngG
p6e2Gpihs03LvbCq8k8P0my9CIm6Ds/DnKAsY0Xn1w13x7AvSrmcyFtHJX0kg0G
nJdbANVOX0oFtxwssUIFvu4TZKaF8MHWUL+rMwbdZPz4tGJnAoIBA0Dpg5Rz1L+Ro
mK6bzcd6LW8yhxvBS12ud0gAyoH4MI2PTElr8wewN8sq7F00Zc75DRq0p4Mzma2CXl
aexqTl1LBQgFctLPsEKYg55S3qnYmN3M6tR5a4kj9HE2183M1fE+Xami3Q+EOHCH
6t+JGyflFAGlmjtgD4c9HlUHKZ042EKwEwFQDbyx750rEj0Ek+a2y0by7y5e7+Y8N
Npbnckv2ufTzjasX17PDzy6rmsUCiPvu0uV/vXHJohHN108vPnxv1FM2jdZUC9C8
5bm5dA70HlPfb+qbppzRf4LABu9Q3TESEXGYLYqM30n6b7R4f81756pnR2NfP
GTxxR99hWJBNAoIBA0DzZPAnXA8rhVfZyEMc/FzjTkyVelbWkbaznAFBh21roJUE
rM9P11bqTUzun0Y38PKxonLNTVhj9ES1Usc8BwWcsyu7dALcNkykQvksMmY717R5
6TFTQ2DCP619r+9NLW3jWGSdLMUJDjuPLBspKD/Lb/MrZ8uZ1x0hZhhdp0ZEYe1n
U/V7gvefABWNPjWKFt1Wjme5ank/zmQ7Izzk3n1f75heB17j+TACF39nG6qm9NCLC
5Spw6c6Hj1vw17p10gKn52gykGLTQgMyUsl+zblH5S1LXGCjDrqFv0crx0Y8L6t1
9LX1x0kgduXc0cDr19a0VCIL8zzUpNRF+yGYPPhTAoIBAQCCEGQ1XvutVsfouHwB9
LIE1voFedR1Xv+red7DCLCT5LvxkFt2D2XhyekIC7FKJ8en08IAmmnQD+9vkkb0b3
9LXsgmFT4baquv9Lc6gmNB1KfcsZb7CJHLkzLxL0uZNMN0AH401x2/Gt1N0HBF
SDbqB8H0yVf8KLELFP33cKSBYMBV1jhtvzCIRLkabzFbpuw1GhyZgTIwLnn29F
2NDE1Y1Y0GurHuIVetyva9w+zS5uyB1g8gLoqhFV/FQFLp8mNKyUxSL9qkwMbc
zLVGFxewibZyXtTgR0FY62ghPkFJTMUMsptwk7Pv3VmxVVO6+T3+81Db1SL/Doen
eB5ZAoIBA0DmHkUcAw6zRCNayt4xnxwCuzczrZruqq0SL7pTNWNDTxeH+zodUvn
v002J2uH3ALuR3/FIXc8A0IBA0D2eHoLwIwKs/RCAxJA1e8grCvqXfFpE9Rk05QA+
8AAP/SeSk/Iw5307H4ba6nsn4XEckVAwqgmJjKJ8JaoUfVeSk5FhmdumnmhLVEtB
aUf5V4xkbend1JzH2COV0QLa8l/cKnILnzrOguHqQ17VUVV5XcQJRG7UVSL19kVY
Ee8B2NzWcFbo5k5tToUqsIhdMuz0G00BGLTGTnQD4vGwyZDrVyFhVqu0yZR7RILC
QKGUhd9QAuuUa3pRrgryGxY30QXESdPZ
-----END PRIVATE KEY-----
```

Ilustración 6 Captura de la clave privada.pem

```

user@user-virtual-machine:~$ cat clave_publica.pem
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA4NJVPVwbry8rkUZQaWv9
rKRYmk6NTp9GCSKjYBv82qS5gN0xTA88apPj7FViEtXgBRGyJcehwPqn0oo2VTbK
0KMbuuEK4noZ008MnZ0r+VP80m2rFtN16v10REpSFHboCtLft31P0nqb0pP3uUI+
+kzS1wum7tT7tXtipcEQBT/07bHY1tHJuJGPK58Fkb2F0ENSVhd1Wd0S5jSdbklB
PZeIcdwgn2/rNzUcActBV19BXxW8nM5Wm+wVITe57uuyw/La8M4iVJWIdZC9xMON
uINYCurBZlnUjv25pPGrtA7gK2MVGwrWx5AgeyUizc7Vs/fEv8aXlTsqsZa77LvG
uqhpCxkkPl608iWFtTqjKWVrbRQIEd0SXMk6o2Bs/ATCsejnmYRM20JUpGLt2L7V
CVV1gYzRtUophwR3lKZFJbC+c4yvXe3XQLPMQV+DAQ/J0DZBr9swsgQhUAYEPd5V
hee9BNwmkn3CXU5x2AA/Jd9QDUtQySlC090RoyJwSOBBdrzejRyQVTmX8/zd6nF
1NPxvKascmHWzj1vKwYaMbRZqWWM6cTcbWib2mKuKBWrrQGxNqA5mcYFyaj6qyjf
BXwo0X5JlkQajn6D6ioC/PvW5o2gM60GKIq+yMKb6Ia20e8SVFqgmErPegccBA5W
GonexQE8vF0x9DLMACADiPsCAWEAAQ==
-----END PUBLIC KEY-----

```

*Ilustración 7 Captura de la clave publica.pem*

Como vemos justo al final de esta última captura el valor del exponente público es 0x10001 o valor 65537. Se sabe al ejecutar el siguiente comando: `openssl rsa -in clave_privada.pem -text | more`

```
publicExponent: 65537 (0x10001)
```

*Ilustración 8 Exponente de la clave pública*

**Pregunta 10.** Imprime en formato texto (parámetro `-text`) todos los parámetros de clave privada generada. El desglose de parámetros, ¿está en hexadecimal o en base64?

Como se aprecia los parámetros de la clave privada generada están en Hexadecimal, esto se sabe porque hexadecimal usa base 16, mientras que base 64 hace uso de 64 valores de representación, en este caso se usa hexadecimal con notación desde 0,1,2,3,4,5,6,7,8,9, A, B, C, D, E, F (16 valores).



```

user@user-virtual-machine:~$ openssl rsa -in clave_privada.pem -text | more
writing RSA key
Private-Key: (4096 bit, 2 primes)
modulus:
 00:e0:d2:55:a5:5c:1b:af:2f:2b:91:46:50:69:6b:
 fd:ac:a4:58:9a:4e:8d:4e:9f:46:09:22:a3:60:1b:
 fc:da:a4:b9:80:d3:b1:4c:0f:3c:6a:93:e3:ec:55:
 62:12:d5:e0:05:11:b2:25:c7:a1:c0:fa:a7:d2:8a:
 36:55:36:ca:d0:a3:1b:ba:e1:0a:e2:7a:19:d3:4f:
 0c:9d:93:ab:f9:53:fc:3a:6d:ab:16:d3:75:ea:fd:
 74:44:4a:52:14:76:e8:0a:d2:c5:b7:7d:4f:3a:7a:
 9b:3a:93:f7:b9:42:3e:fa:4c:d2:d7:0b:a6:ee:d4:
 fb:b5:7b:62:a5:c1:10:05:3f:ce:ed:b1:d8:d6:d1:
 c9:b8:91:8f:93:9f:05:91:bd:85:38:43:52:56:17:
 75:59:dd:12:e6:34:9d:6e:49:41:3d:97:88:71:dc:
 20:9f:6f:eb:37:35:1c:01:cb:41:57:5f:41:5f:15:
 bc:9c:ce:56:9b:ec:15:21:37:b9:ee:eb:b2:c3:f2:
 da:f0:ce:22:54:95:88:75:90:bd:c4:c3:8d:b8:83:
 58:0a:ea:c1:66:59:d4:8e:fd:b9:a4:f1:ab:b4:0e:
 e0:2b:63:15:1b:0a:d6:c7:90:20:7b:25:22:cd:ce:
 d5:b3:f7:c4:bf:c6:97:95:3b:2a:e5:96:bb:ec:bb:
 c6:ba:a8:69:0b:19:24:3e:5e:b4:f2:25:85:b5:3a:
 a3:29:65:6b:6d:14:08:11:d3:92:5c:c9:3a:a3:60:
 6c:fc:04:c2:b1:e8:e7:99:84:4c:d8:e2:54:a4:62:
 ed:d8:be:d5:09:55:75:81:8c:d1:b5:4a:29:87:04:
 77:94:a6:45:25:b0:be:73:8c:af:5d:ed:d7:40:b3:
 cc:41:5f:83:01:0f:c9:d0:36:41:af:db:30:b2:04:
 21:50:06:04:3d:de:55:85:e7:bd:04:dc:26:92:7d:
 c2:5d:4e:71:d8:00:3f:25:df:50:0d:4b:50:c9:29:
 42:3b:d3:91:a3:22:70:48:e0:41:6d:da:f3:7a:34:
 72:41:54:e6:5f:cf:f3:77:a9:c5:d4:d3:f1:bc:a6:
 ac:72:61:d6:ce:3d:6f:2b:06:1a:31:b4:59:a9:65:
 8c:e9:c4:dc:6d:62:1b:da:62:ae:28:15:ab:ad:01:
 97:36:a0:39:99:c6:05:c9:a8:fa:ab:28:df:05:7c:
 28:d1:7e:49:96:44:1a:8e:7e:83:ea:2a:02:fc:fb:
 d6:e6:8d:a0:33:ad:06:2a:2a:be:c8:c2:9b:e8:86:
 b6:d1:ef:12:54:5a:a0:98:4a:cf:7a:07:1c:04:0e:
 56:1a:89:de:c5:01:3c:bc:53:b1:f4:32:cc:00:20:
 03:88:fb
publicExponent: 65537 (0x10001)

```

*Ilustración 9 Captura 1 con detalles clave privada.pem en formato texto*

```

privateExponent:
  10:48:81:00:d9:0a:fd:9a:8d:02:98:9f:cf:ad:8d:
  51:fe:6a:97:17:d9:64:38:64:fa:2f:12:bb:83:4b:
  6d:0a:96:8f:9e:1a:d9:47:6b:e3:76:e8:00:80:ae:
  a4:6e:99:2b:1a:27:ac:ff:7d:d7:b1:a5:36:0f:e1:
  f4:df:63:11:24:14:7e:14:8e:95:43:58:06:2b:53:
  89:40:de:29:26:21:69:44:9d:7f:a9:bb:d5:fe:9a:
  cd:2c:bf:85:26:97:92:86:71:8b:8d:fd:39:b4:67:
  9f:21:2d:c5:5d:3c:47:cf:5d:f5:f5:57:6c:8a:40:
  86:2f:1e:eb:4d:1b:11:46:43:2b:de:c0:60:79:66:
  ad:82:32:c3:f3:b5:e8:e3:06:78:6c:bd:29:e9:c9:
  0b:6e:82:4f:ea:14:fc:f2:91:51:c4:b2:92:8c:94:
  50:4d:40:31:5f:72:07:d9:e6:2c:4d:d9:e3:93:cf:
  75:61:51:cf:39:3f:79:33:1a:b9:bd:ed:d4:ae:0c:
  ed:79:55:ed:df:bc:0d:1d:23:f6:d1:b3:12:0a:1b:
  f6:59:1f:be:2a:03:70:82:85:4f:a2:5c:02:a3:e6:
  83:3d:f4:94:0b:7f:98:34:a2:d0:48:80:47:7d:13:
  92:aa:aa:0a:b9:cc:d6:22:28:43:e3:5c:4e:69:20:
  9b:81:93:63:38:77:ec:7b:4f:51:d8:49:72:c7:a2:
  14:41:08:84:eb:7f:71:66:f6:fa:97:9f:0a:e7:d2:
  d6:33:93:1a:7d:3c:20:00:5e:57:2b:6d:7d:60:84:
  9b:d0:3e:56:2b:65:ce:ad:51:81:b4:a0:e7:17:9a:
  c3:58:5a:98:67:3a:82:69:b6:ff:11:c8:4e:75:7b:
  10:40:81:31:f1:e0:3e:ca:bf:3d:38:5a:f0:e3:c5:
  df:62:2d:eb:d9:93:e5:0b:6c:c7:5f:bb:97:70:13:
  1d:30:8c:06:af:7f:ae:13:79:c5:d2:05:9e:5e:c3:
  8f:39:d1:f9:31:34:df:b9:5c:ea:f3:e6:7b:05:be:
  d6:49:42:72:d8:36:68:02:f4:6b:8b:a1:18:a1:6d:
  09:76:b6:0c:80:ca:55:6e:69:c2:10:dd:95:4c:9c:
  77:18:57:a4:e9:5c:11:23:48:14:04:f6:c3:ae:63:
  1a:d1:79:0a:ff:15:96:df:68:0d:b7:8f:ab:ce:af:
  f0:5f:5d:ae:1b:15:51:be:86:a4:8c:26:88:40:56:
  01:ae:09:59:b8:05:8c:00:f1:08:e7:e4:13:30:f0:
  9e:35:2f:1e:19:03:02:f2:b6:21:00:35:bb:dd:eb:
  49:2e:43:bb:a8:43:5b:87:dc:02:6c:47:7f:c5:21:
  77:01
prime1:
  00:f6:78:7a:08:c2:29:2c:fd:10:80:c4:90:35:7b:
  c8:2b:1a:fa:97:7c:5a:44:f5:19:10:b1:00:3e:f0:
  06:8f:fd:27:92:2b:f2:30:e7:7d:3b:1f:86:da:ea:
  7b:27:e1:71:1c:91:50:30:ab:a9:89:8c:a2:7c:25:
  aa:14:7d:57:92:93:91:61:98:3b:a6:9e:68:65:bc:
  4b:41:56:ff:11:90:ff:2b:f8:d0:4d:3b:2d:e3:12:
  1c:8a:73:36:ef:5e:e8:f6:40:2a:be:56:d5:cc:23:
  dd:11:ed:e2:85:2e:72:48:68:ef:7f:b1:7c:6f:82:
  8d:5d:a2:05:56:c0:a0:aa:06:cc:bc:a2:a9:62:12:
  d5:5d:c9:76:73:fb:16:65:2a:b8:49:10:c0:6a:9f:
  51:01:cf:ca:86:ce:39:c5:36:f3:fb:e4:f9:26:c7:
  fe:ce:35:16:63:9c:6b:20:a7:a7:b6:1a:98:a1:b3:
  4d:cb:bd:b0:aa:2b:c9:3c:3c:e9:b2:d0:22:26:e8:
  3b:3f:0e:72:80:b1:8d:17:9e:5c:35:df:1e:c0:bd:
  2a:e6:73:21:6d:1c:95:ce:92:0d:06:9e:30:db:00:
  d5:4e:5f:4a:05:b7:1c:2c:49:42:1f:be:ee:13:64:
  a6:9f:f0:c1:d6:52:5f:ab:33:06:c3:64:fc:f8:b4:
  62:67

```

*Ilustración 10 Captura 2 con detalles clave privada.pem en formato texto*



```

prime2:
00:e9:83:94:73:97:e4:68:98:ae:9b:cd:c7:7a:89:
66:3c:ca:15:ef:f1:22:36:b8:38:00:ca:81:f8:30:
8d:8f:4e:d9:6b:f3:07:96:37:ca:bb:17:4d:19:73:
be:43:46:aa:1b:31:99:9a:d8:25:e2:69:ec:6a:4e:
29:65:05:08:1f:72:d9:4f:b0:42:98:83:9e:52:26:
a9:d8:32:7d:cc:ea:d4:79:6b:89:23:f4:71:36:d7:
cd:cc:89:f1:3e:5d:a9:a2:dd:0f:84:a0:77:07:ea:
df:89:1b:27:c5:82:29:a3:b6:00:f8:73:d8:48:50:
79:19:d3:8d:84:2b:01:30:15:00:db:cb:1e:f9:d2:
b1:23:39:e2:be:6b:6c:8e:6f:2e:f2:e5:ee:dd:f9:
8f:0d:36:96:e7:72:4b:f6:b8:5b:59:8d:ab:17:d7:
b3:c3:cf:2e:ab:9a:c5:02:88:fb:ee:3a:e5:7f:bd:
71:c9:a2:11:cd:94:ef:2f:3e:7c:72:bf:51:4c:da:
3c:d4:0b:d0:bc:e5:b9:92:74:0e:f4:1e:2a:5f:6f:
ea:9b:a6:9c:d1:7f:82:c0:6e:ef:50:dd:31:12:7b:
11:06:61:76:0b:ca:a3:37:a2:7e:9b:ed:1e:1f:f3:
5e:f9:ea:99:d1:cc:d1:69:18:8c:57:47:df:61:58:
90:4d
exponent1:
00:f3:64:f0:26:5c:0f:2b:85:51:59:c8:43:1c:fd:
fb:23:4e:46:2f:78:b6:f0:28:16:b3:9c:07:c1:1f:
69:6b:a2:35:04:ad:6f:43:8a:26:ea:4e:ec:ee:9c:
e6:37:f0:f2:b1:a2:72:cd:4d:88:63:f4:44:b5:52:
c0:8d:f1:65:9c:b3:2b:bb:74:09:5c:36:4c:a4:42:
f9:12:32:66:3b:23:b4:49:e9:31:53:43:60:c2:3f:
ad:7d:af:df:8d:2d:6d:e3:58:64:9d:88:c5:23:0e:
3b:8f:2c:1b:29:28:3f:e5:6f:f3:2b:67:cb:99:97:
14:21:66:11:dd:a4:e6:44:61:e8:a7:53:fe:ef:81:
e7:c0:f1:65:8f:8d:62:85:4f:55:a3:99:ee:5a:9c:
af:f3:99:0e:c8:67:39:37:9f:57:fb:e6:17:81:8b:
b8:fe:4c:00:ab:27:d9:c6:ea:a9:bd:34:b0:8b:e6:
b4:a9:c1:ce:87:8e:2b:f0:d7:ba:75:42:02:a7:e7:
68:32:92:02:d3:42:03:32:52:c9:7e:cd:b2:e1:e5:
2d:4b:5c:60:a3:0e:ba:85:bf:47:2b:c4:e6:3c:2f:
ab:75:f4:b5:f5:c4:e9:06:76:e5:dc:d1:c0:eb:d7:
d6:90:55:c2:25:f3:3c:d4:a4:d4:45:fb:21:b2:3c:
f8:7b
exponent2:
00:84:19:0d:57:be:eb:55:48:5a:2e:85:60:7d:2f:
51:08:be:81:5e:75:18:97:bf:ea:de:77:b0:c2:88:
24:ec:96:fc:64:16:dd:89:db:11:f2:78:a2:02:ed:
f9:09:f1:e5:b4:f0:80:26:9a:74:03:fb:4b:e4:6f:
46:f7:80:bb:31:9f:34:d3:e1:b0:2a:ba:fa:4b:1a:
d8:26:17:9a:16:dc:19:4a:7e:cc:db:ec:22:47:96:
19:33:c6:2d:14:cc:c3:74:00:7e:10:d6:fd:bf:1a:
dd:4d:a0:71:05:48:36:ea:07:c1:d0:cb:27:e4:f0:
b1:31:2c:fd:f7:70:a4:81:60:c0:55:96:38:75:b6:
fc:c2:22:b2:e4:69:bc:c5:6e:9c:2e:88:68:72:66:
04:c8:c2:c2:e7:37:3f:45:d8:d0:c4:7e:61:f5:60:
ee:ae:ac:7b:88:54:4b:72:bd:af:56:fb:36:6c:e6:
ec:81:d6:0f:20:2f:4a:87:7d:5f:c5:41:f9:69:f2:
63:4a:c9:4c:52:2f:da:a4:c0:c6:dc:ce:5b:c6:15:
77:b0:89:b6:58:c5:3b:60:44:e1:58:eb:68:21:3e:
41:49:4c:c5:0c:b2:9b:56:93:b3:ef:dd:59:97:55:
83:ba:f9:3d:fe:f3:50:db:95:29:7f:0e:87:8d:78:
1e:59

```

Ilustración 11 Captura 3 con detalles clave privada.pem en formato texto

```

coefficient:
00:e6:1c:a5:1c:03:0e:b3:c5:10:8d:6b:2b:78:c6:
7c:17:72:ec:dc:ce:bc:eb:ba:aa:8e:4a:5e:e9:4c:
d5:8d:0d:3c:5e:87:ec:e8:75:4b:e7:bf:ad:19:8d:
90:f4:23:33:3a:c9:bd:9d:9b:d3:b3:49:c1:e7:ab:
2a:85:73:ae:78:1a:b3:9a:da:04:ed:c2:71:8c:48:
b1:62:56:19:a8:05:40:7e:f6:6e:e8:62:91:dd:66:
23:5b:53:6a:42:9c:9c:ec:0d:e3:b5:43:54:ff:1d:
05:f6:42:09:46:03:19:31:01:68:a1:3b:8f:e3:65:
56:e5:0a:c9:35:f1:c7:af:87:37:c9:5b:5c:f5:82:
c8:ab:6a:e1:79:57:85:e4:6c:49:dd:d4:9c:c7:d8:
23:95:d1:09:5a:f2:2f:dc:2a:72:25:37:3a:ce:1a:
e8:50:80:8e:d5:bd:45:6c:5d:c8:09:46:0e:d4:55:
22:e2:f6:45:58:11:ef:01:d8:dc:d6:71:f6:e8:e6:
4e:6d:4e:85:2a:b0:88:5d:32:ec:ce:1a:8d:01:18:
b4:c6:4e:74:03:e2:f1:b0:cb:30:d1:bf:21:61:be:
ab:8e:c9:94:7b:44:89:42:40:a1:94:85:df:50:02:
eb:94:6b:7a:51:ae:0a:f2:1b:16:37:a1:05:c4:b1:
d3:d9

```

Ilustración 12 Captura 4 con detalles clave privada.pem en formato texto

```

-----BEGIN PRIVATE KEY-----
MIIEJRAIBADANBgkqhkiG9w0BAQEFAASCCS4wggkqAgEAAoICAQDg0LwLXBuvLyuR
RLBpa/2spFiaTo1On0YJIqNgG/zapLmA07FMDzxqk+PsVWIS1eAFEBILx6HA+qfS
ijZVNSrQoxu64QrIehnTTwydk6v5U/w6basW03Xq/XRESLIUdugK0sW3fU86eps6
k/e5Qj76TNLXC6bu1Pu1e2KLwRAFP87tsdjW0cm4kY+TnwWRvYU4Q1JWF3VZ3RLM
NJ1uSUE9L4hx3CCfb+s3NRwBy0FFX0FFbyszLab7BUHN7nu67LD8trwziJULYh1
kL3Ew424g1gK6sFmWdSO/bmk8au0DuArYxUbCtbHkCB7JSLNztWz98S/xpeV0yrl
lrvsu8a6qGKLGSQ+XrTyJYw10qMpZWttFagR05JcyTqjYGz8BMKx60eZhEzY4LSk
Yu3YvtUJVVXBWjNG1SImHBHeUpkULsL5zjK9d7ddAs8xBX4MBD8nQNKGV2zCyBCFQ
BgQ93LWF570E3CaSfcJdTnHYAD8L31ANS1DJKUI705GjInBI4EFt2vN6NHJBVOzf
z/N3qcXU0/G8pqxyYdb0PW8rBhoxTFmpZYzpxNxtYhvaYq4oFautAZc2oDmZxgXJ
qPqrKN8FFcJrFkmWRBqOfopqKgL8+9bmjaAzrQYqKr7IwpvohrBR7xJUWqCYS96
BxwEDLYaid7FATy8U7H0MswAIAOI+wIDAQABAoICABBIgQDZCv2ajQKYn8+tjVH+
apcX2WQ4Z2PovEruD520KLo+eGtLHa+N26ACArqRumSsaJ6z/fdexpTYP4fTFYEk
FH4UjpVDWAYrU4LA3ikmIwLEnX+pu9X+ms0sv4Uml5KGcYuN/Tm0Z58hLcVdPEfP
XfX1V2yKQIYvHutNGxFGQyvevGB5Zq2CMsPztejjBnhsVSnpyQtugk/qFPzykYr
spKM1FBNQDFcgcgZ5ixN2e0Tz3VhUc85P3kzGrm97dSuD015Ve3fva00I/bRxsIK
G/ZZH74qA3CCHU+IXAKj5oM99JQLf5g0otBIEgEd9E5Kqggq5zNYiKEPjXE5pIJuB
k2M4d+X7T1HYSLHohRBCITrf3Fm9vqXnwrn0tYzKxp9PCAAXLcxbX1ghJvQPLYr
Zc6tUYG0oOcXmsNYWphn0oJptv8RyE51exBAgThx4D7Kvz04Wvdjxd9iLevZk+UL
bMdfu5dwEx0wjAavf64TecXSBZ5ew4850fKxNN+5XOrz5nsFvtZJQnLYNmG9GcuL
oRihbQL2tgyAylVuacIQ3ZVMnHcYV6TpXBEjSBQe9sOuYxrReQR/FZbfaA23j6v0
r/BfXa4bFVG+hqSMJohAVgGuCvM4BYwABQjn5BMw8J41Lx4ZAwLytiEAnbvde0ku
Q7uo01uH3AJ3R3/FIXcBAoIBAQD2eHoIwIks/RCAXJA1e8grGvqXfFpE9RkQsQA+
8AaP/SeSK/Iw5307H4ba6nsn4XEckVAwq6mJjKJ8JaoUfVeSk5FhmDumhmlVetB
Vv8RKP8r+NBNOy3jEhyKczbvXuJ2QCq+VtXMI90R7eKFLnJIA09/sXxvgo1dogVW
wKcQbsy8oqliEtVdyXZz+XZlKrHJEMBqn1EBz8qGzjnFNvp75Pkmx/7ONRZjnGsg
p6e2Cpihs03LvbCqK8k8Pomy0CIm6Ds/DnKAsY0Xnlw13x7AvSrmcyFTHJX0kg0G
nJDbANVOX0oFtxwsSUIfvu4TZKaf8MHwUL+rMwBDZPz4tGJnAoIBAQQDp5RzL+Ro
mK6bzcd6iWY8yhXv8SI2uBgAyoH4MI2PTtlr8weWN8q7F00Zc75DRqobMZma2CXi
aexqTillBQgfcTLpsEKYg55JqnYmN3M6tR5a4kj9HE2183MiFE+Xami3Q+EoHch
6t+JGyFfGtmjtgD4c9hIUHkZ042EKwEwFQDbyx750rEj0eK+a2yOby7y5e7d+Y8N
Npbnckv2uFtZjasX17PDzy6rmsUCiPvuOuV/vXHJohHNL08vPnxxyv1FM2jzUC9C8
5bmSdA70HiPfb+qbppzRf4LABu9Q3TESexEGYXYLYqM3on6b7R4f81756pnRzNfp
GIxXR99hWJBNAoIBAQQDzZPAMXA8rhVFZyEMc/fsjTkYveLbwKBaznAFBH2lroJUE
rW9DiibqTuzun0Y38PKxonLNTYhj9ES1UsCN8Wwcsyu7dAlcNkykQvkSMmYI7Rj
6TFTQ2DCP619r9+NLW3jWGSdIMUjDjuPLBspKD/Lb/MrZ8uZLxQhZhdHpoZEYEIn
U/7vgefA8WwPjWKFt1WjmeSanK/zmq7Izzk3n1f75heBi7j+TACrJ9nG6qm9NLCL
5SpwcFmH1V06urHuIVETyva9W+zzs5uyB1g8gL0qHfV/FQflp8mNKyUxSL9qkwMbc
zlvGFXewibZYxTtgR0FY62ghPkFJTMUMsptWk7Pv3VmXVY06+T3+81DbLSL/Doen
eB5ZAoIBAQMhMKUcAw6zxRCNayt4xnxWcuzczrzruqq0SL7pTNWNDTxeH+zodUvn
v60ZjZD0IzM6yb2dm90zScHnqyqFc654Gr0a2gtwnGMSLFiVhmoBUB+9m7oVpHd
ZiNbU2pCnJzsDe01Q1T/HQX2QqLGAXkxAWih04/jZVbLcSk18cevhzFJW1z1qisrY
auF5V4XkbEnd1JzH2COV0Qla8i/cKnILNzrOGuhQgI7VvUvXcXgJRgU7VSL9kVY
Ee8B2NzWcfbo5k5tToUqsIhdMuZOG00BGLTGTnQD4vGwyZDRvyFhvqu0yZR7RILC
QKGUhd9QAuuUa3PrRgryGxY3oQXESdPZ
-----END PRIVATE KEY-----

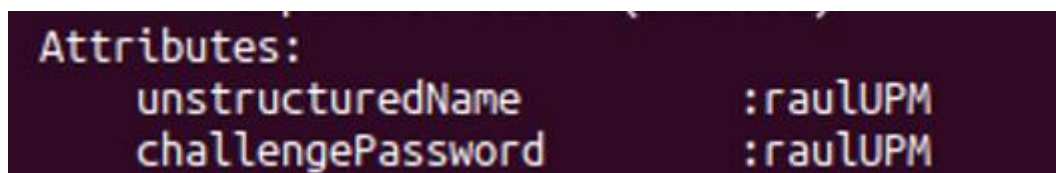
```

Ilustración 13 Captura 5 con detalles clave privada.pem en formato texto

## 2. Obtención de credenciales

Pregunta 11. ¿Qué es la Challenge Password que se solicita, de forma opcional, durante el proceso de creación de la petición? Pista: está definido en la RFC 2985.

Según la RFC 2985, la challenge password es una contraseña que permite a una entidad solicitar la revocación la petición del certificado.



*Ilustración 14 Captura Challenge Password*

Pregunta 12. ¿Qué versión de certificado ha creado? ¿Qué algoritmo para firma se ha usado? ¿Qué fechas de validez tiene? ¿Es válido desde el mismo momento en que se crea o desde el día siguiente?

La versión del certificado utilizada es la versión 1, el algoritmo de firma utilizado es sha256withRSAEncryption, la fecha de validez es de exactamente un año y el certificado comienza a ser válido en el momento en el que se crea el certificado. Se aprecia todo esto en las capturas siguientes para este apartado.

Antes de generar el certificado, se debe generar la petición de certificado, para después la CA o Autoridad de Certificación pueda generar el certificado a partir de dicha petición de certificado.

En este apartado se va a mostrar tanto la creación de una petición de certificado como la posterior creación de un certificado digital por parte de la Autoridad de Certificación a partir de dicha petición de certificación.

Previamente se ha creado el par de claves para el usuario “normal”, pero ahora se debe generar también un par de claves para la autoridad de certificación ya que esta para crear el certificado debe firmar con su clave secreta dicho certificado. La petición de certificación por su parte va firmada con la clave secreta de la entidad que realiza la solicitud, en este caso con la clave secreta del primer par de claves generado.



```

user@user-virtual-machine:~$ openssl req -new -key clave_privada.pem -out peticion.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPM
Organizational Unit Name (eg, section) []:Servidores
Common Name (e.g. server FQDN or YOUR name) []:Raul
Email Address []:raul.calderon.moya@alumnos.upm.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:raulUPM
An optional company name []:raulUPM

```

*Ilustración 15 Captura proceso de creación de una petición de certificación*

```

user@user-virtual-machine:~$ openssl req -text -in peticion.csr
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:e0:d2:55:a5:5c:1b:af:2f:2b:91:46:50:69:6b:
        fd:ac:a4:58:9a:4e:8d:4e:9f:46:09:22:a3:60:1b:
        fc:da:a4:b9:80:d3:b1:4c:0f:3c:6a:93:e3:ec:55:
        62:12:d5:e0:05:11:b2:25:c7:a1:c0:fa:a7:d2:8a:
        36:55:36:ca:d0:a3:1b:ba:e1:0a:e2:7a:19:d3:4f:
        0c:9d:93:ab:f9:53:fc:3a:6d:ab:16:d3:75:ea:fd:
        74:44:4a:52:14:76:e8:0a:d2:c5:b7:7d:4f:3a:7a:
        9b:3a:93:f7:b9:42:3e:fa:4c:d2:d7:0b:a6:ee:d4:
        fb:b5:7b:62:a5:c1:10:05:3f:ce:ed:b1:d8:d6:d1:
        c9:b8:91:8f:93:9f:05:91:bd:85:38:43:52:56:17:
        75:59:dd:12:e6:34:9d:6e:49:41:3d:97:88:71:dc:
        20:9f:6f:eb:37:35:1c:01:cb:41:57:5f:41:5f:15:
        bc:9c:ce:56:9b:ec:15:21:37:b9:ee:eb:b2:c3:f2:
        da:f0:ce:22:54:95:88:75:90:bd:c4:c3:8d:b8:83:
        58:0a:ea:c1:66:59:d4:8e:fd:b9:a4:f1:ab:b4:0e:
        e0:2b:63:15:1b:0a:d6:c7:90:20:7b:25:22:cd:ce:
        d5:b3:f7:c4:bf:c6:97:95:3b:2a:e5:96:bb:ec:bb:
        c6:ba:a8:69:0b:19:24:3e:5e:b4:f2:25:85:b5:3a:
        a3:29:65:6b:6d:14:08:11:d3:92:5c:c9:3a:a3:60:
        6c:fc:04:c2:b1:e8:e7:99:84:4c:d8:e2:54:a4:62:
        ed:d8:be:d5:09:55:75:81:8c:d1:b5:4a:29:87:04:
        77:94:a6:45:25:b0:be:73:8c:af:5d:ed:d7:40:b3:
        cc:41:5f:83:01:0f:c9:d0:36:41:af:db:30:b2:04:
        21:50:06:04:3d:de:55:85:e7:bd:04:dc:26:92:7d:
        c2:5d:4e:71:d8:00:3f:25:df:50:0d:4b:50:c9:29:
        42:3b:d3:91:a3:22:70:48:e0:41:6d:da:f3:7a:34:
        72:41:54:e6:5f:cf:f3:77:a9:c5:d4:d3:f1:bc:a6:
        ac:72:61:d6:ce:3d:6f:2b:06:1a:31:b4:59:a9:65:
        8c:e9:c4:dc:6d:62:1b:da:62:ae:28:15:ab:ad:01:
        97:36:a0:39:99:c6:05:c9:a8:fa:ab:28:df:05:7c:
        28:d1:7e:49:96:44:1a:8e:7e:83:ea:2a:02:fc:fb:
        d6:e6:8d:a0:33:ad:06:2a:2a:be:c8:c2:9b:e8:86:
        b6:d1:ef:12:54:5a:a0:98:4a:cf:7a:07:1c:04:0e:
        56:1a:89:de:c5:01:3c:bc:53:b1:f4:32:cc:00:20:
        03:88:fb
      Exponent: 65537 (0x10001)
  Attributes:
    unstructuredName :raulUPM
    challengePassword :raulUPM
  Requested Extensions:
  Signature Algorithm: sha256WithRSAEncryption

```

*Ilustración 16 Captura 1 peticion.csr en modo texto*

Signature Value:

b9:98:dc:60:4c:f8:d3:fa:0f:f6:2c:89:f9:2c:0e:ff:e3:18:  
12:e0:25:61:3c:e8:e4:1a:3f:f2:73:d7:d1:a3:0f:06:3a:47:  
40:c6:30:4b:d3:b9:fd:ca:81:71:5e:09:6b:15:00:da:fe:a3:  
fd:62:81:b8:cb:4d:80:0b:29:ad:dd:f2:c6:d0:e0:49:83:44:  
38:a8:ed:d9:27:e7:ce:5c:1e:24:fb:df:df:6a:77:36:76:ad:  
99:65:ff:72:b0:14:5f:7f:6f:43:d8:4f:a8:9c:09:66:25:7d:  
06:98:84:d3:6c:bc:75:bf:1e:be:3f:40:eb:67:06:16:1e:36:  
de:25:4a:45:45:05:97:0e:85:0b:c4:2f:6c:00:30:dd:18:39:  
ff:8b:04:d5:9c:e7:86:b7:13:05:a5:92:0d:d5:b3:6d:80:bd:  
5c:58:45:f6:35:12:59:d4:55:e8:19:f7:f7:6f:86:41:bc:aa:  
64:fe:fe:2c:5e:21:dd:e8:69:c2:7d:5a:67:fd:72:0b:11:a7:  
64:b7:6c:e4:9f:66:dc:99:bb:33:86:0a:23:f8:7e:2f:e5:04:  
63:3f:d7:4c:b3:57:17:e6:a4:c8:07:e9:e7:86:9a:51:e3:c1:  
40:9b:f7:2a:16:22:6d:e9:46:0f:8c:c4:93:2b:89:9a:b2:4e:  
03:e3:f7:d9:6f:73:81:91:ce:7b:d2:46:87:4a:0c:f1:68:4b:  
85:fd:39:8f:2d:ca:f7:b5:2e:5f:87:82:7a:50:b4:3c:5f:d4:  
7d:2f:98:f0:6f:e3:7f:ea:19:d0:06:d7:2b:88:f5:39:e7:73:  
98:26:a9:89:4e:d4:1c:ac:f2:95:e4:69:cc:87:4c:5a:e3:7e:  
d5:ff:2c:ea:56:f5:82:b6:88:e2:99:51:d1:9c:9b:77:cf:02:  
97:7f:fd:a4:83:f0:8b:69:e1:0b:e2:33:f7:98:eb:d2:5f:c4:  
59:fa:d9:f2:dd:9c:6f:5e:b7:f6:39:ce:19:b7:ab:d9:13:3b:  
f0:4e:31:2b:7b:e4:fb:5c:8e:a0:41:a1:28:3e:7e:c7:e5:f4:  
67:ae:d8:4c:88:aa:91:04:b9:bb:cb:4d:59:b6:d3:99:69:7a:  
b7:6f:8a:55:1c:53:da:66:23:3f:8a:ff:ef:73:65:08:92:5c:  
38:87:3a:a4:f0:1a:cf:cd:a9:7e:a5:61:94:bc:53:4e:66:62:  
9b:7e:51:26:d9:86:be:27:04:8a:95:ca:19:1e:a1:a5:c8:3d:  
67:c8:05:42:7d:f2:13:ed:f9:60:c0:7e:68:86:49:8a:a7:5e:  
61:f4:ec:54:44:63:ad:04:b7:1a:c1:b2:f3:9c:11:a9:00:42:  
88:81:f3:63:90:60:45:14

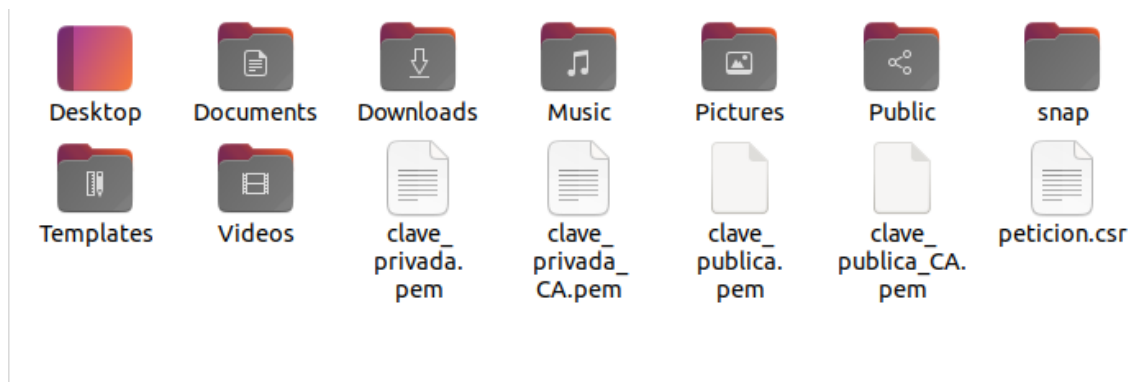
-----BEGIN REQUEST-----

MIIFCTCCAvECAQAwgZMxCzAJBgNVBAYTAKVTMQ8wDQYDVQQIDAZNYWRyaWQxZDZANBgNVBACMBk1hZHJpZDEMMoGA1UECgwDVVBNNMRMwEQYDVQQLDAPtZXJ2aWRvcmlVzMQ0wCwYDVQQDDARSYXVsMTAwLgYJKoZIhvcNAQkBFiFyYXVsLmNhbGRlcm9uLm1vZWFAWw1bW5vcy51cG0uZXNwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDg0lWLBuvLyuRRlBpa/2spFiaTo10n0YJIqNgG/zapLmA07FMDzxqk+PsVWIS1eAFEBilx6HA+qfSijZVNsRQoxu64QriehnTTwydk6v5U/w6basW03Xq/XRESliUdugK0sW3FU86eps6k/e5Qj76TNLXC6bu1Pu1e2KlwRAFP87tsdjW0cm4kY+TnwWRvYU4Q1JWF3VZ3RLmNJ1uSUE9L4hx3CCfb+s3NRwBy0FXX0FFbyczlab7BUHn7nu67LD8trwziJULYh1kL3Ew424g1gK6sFmWdS0/bmk8au0DuArYxUbCtbHkCB7JSLNztWz98S/xpeV0yrllrvsu8a6qGkLGSQ+XrTyJYW10qMpZWttFagR05JcyTqjYGz8BMKx60eZhEzY4lSkYu3YvtUJvXWBJNG1SimHBHeUpkUlsL5zjk9d7ddAs8xBX4MBD8nQNKgV2zCyBCFQBgQ93lWF570E3CaSfcJdTnHYAD8l31ANS1DJKUI705GjInBI4Eft2v6NHJBVOZfz/N3qcXU0/G8pqxyYdb0PW8rBhoxTFmpZYzpxNxtYhvaYq4oFautAZc2oDmZxgXJqPqrKN8FfcjRfkmWRBq0foPqKgL8+9bmjaAzrQYqKr7IwpvohrbR7xJUWqCYSS96BxwEDLYaid7FATy8U7H0MswAIAOI+wIDAQABOAwFgYJKoZIhvcNAQkCMQkMB3JhdWxVUE0wFgYJKoZIhvcNAQkHMqMB3JhdWxVUE0wDQYJKoZIhvcNAQELBQADggIBALmY3GBM+NP6D/YsifksDv/jGBLgJWE860QaP/Jz19GjDwY6R0DGMevTuf3KgXFeCwsVANr+o/1igbjLTYALKa3d8sbQ4EmDRDio7dkn585ChiT7399qdzZ2rZll/3KwFF9/b0PYT6icCWYlfQaYhNNsvHW/Hr4/Q0tnBhYeNt4lSkVF BZc0hQvEL2wAMN0YOf+LBNWc54a3EwWlkg3Vs22AvVxYRfY1ElNUVegZ9/dvhkG8qmT+/ixeId3oacJ9Wmf9cgsRp2S3b0SfZtyZuz0GciP4fi/LBGM/10yzVxfmpMgH6eeGmlHjwUCb9yowIm3pRg+MxJMriZqyTgPj99lvc4GRznvSRodKDPFoS4X90Y8tyve1Ll+HgpnQtDxf1H0vmPBv43/qGdAG1yuI9Tnnc5gmqYl01Bys8pXkacyHTFrjftX/L0pw9YK2iOKZUdGcm3fPAPd//aSD8Itp4QvIM/eY69JfxFn62fLdnG9et/Y5zhm3q9kTO/B0MSt75PtcjqBBoSg+fsfL9Geu2EyIqpEEubvLTvm205lperdvilUcU9pmIz+K/+9zZQiSXDih0qTwGs/NqX6LYZS8U05mYpt+USbZhr4nBIqVyhkeoaXIPWfIBUJ98hPt+WDAfmiGSYqnXmH07FREY60EtxrBsv0cEakAQoiB820QYEUU

Ilustración 17 Captura 2 petición.csr en modo texto



De tal modo que, al crear otro par de claves, quedan los siguientes documentos creados:



*Ilustración 18 Captura con los archivos generados a partir de los comandos*

```
user@user-virtual-machine: $ openssl genrsa -out clave_privada_CA.pem 4096
user@user-virtual-machine: $ openssl rsa -in clave_privada_CA.pem -pubout -out clave_publica_CA.pem
writing RSA key
user@user-virtual-machine: $ openssl x509 -req -days 365 -in peticion.csr -signkey clave_privada_CA.pem -out certificadoCreado.crt
Certificate request self-signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
```

*Ilustración 19 Creación de un certificado a partir de la clave privada de la CA y de la petición de certificación*

En la captura anterior, figura el proceso de creación de claves para la CA y también la generación de un certificado digital a partir de la petición de certificación que va firmada por la clave secreta del solicitante y luego el certificado que va firmado por la clave secreta de la autoridad de certificación.

Ahora, se va a mostrar el certificado con el fin de demostrar que realmente dicho certificado generado se ha realizado correctamente y vemos que tiene un periodo de validez respecto el momento en el que fue creado.

```

user@user-virtual-machine:~$ openssl x509 -in certificadoCreado.crt -text
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      0f:99:d2:74:52:86:ca:2f:c0:89:0d:9c:8c:3c:c3:ef:f3:3d:b2:79
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
    Validity
      Not Before: Apr 27 20:21:17 2024 GMT
      Not After : Apr 27 20:21:17 2025 GMT
    Subject: C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:db:32:fc:b5:c7:02:22:70:58:01:93:a9:d9:80:
        25:e4:6f:4d:d2:67:76:03:6a:50:3f:59:aa:c2:92:
        5a:c7:c4:35:1c:47:bf:52:76:8b:d7:70:9e:7b:df:
        ab:c9:07:df:46:7e:5f:ea:89:63:c6:81:06:77:4d:
        f3:61:28:8c:9f:06:1e:4f:41:b7:99:d5:f3:11:9b:
        b4:a1:9b:f1:b8:4f:3a:55:2b:75:f5:7c:d0:a0:48:
        02:6d:90:dd:55:6f:e2:b4:5d:23:45:e4:e9:64:0c:
        14:61:1e:63:f6:f3:74:55:f8:0b:44:44:f2:35:03:
        c6:29:42:dc:c7:ec:e2:38:09:b2:ef:ad:2f:36:d9:
        ba:f2:d8:65:83:d7:f8:c4:d4:d4:35:8d:dd:e7:bc:
        c3:d4:5d:8e:38:2a:05:46:2e:37:56:f7:30:3a:e2:
        41:50:95:02:1d:74:73:cf:b7:5b:2c:1d:44:2f:c7:
        c1:6b:f3:4d:53:74:3a:dc:49:af:5e:59:fe:64:19:
        26:a4:d1:83:b7:03:bf:50:bc:48:e8:89:e0:d6:ad:
        d4:b4:be:8d:f4:9b:e5:f5:2b:2f:1d:26:d3:bc:29:
        b5:9d:75:e7:67:60:91:1c:00:b1:9e:fc:01:1e:fb:
        76:b3:3a:7a:49:9f:62:cb:4f:3c:c6:4b:bc:5f:6a:
        71:e9:f6:ef:cd:3f:94:4e:9d:18:12:4c:75:b4:06:
        d9:72:ad:70:04:f5:38:44:13:3e:87:41:06:6a:46:
        5e:0c:c1:7d:b4:e0:a3:53:c6:81:e7:57:f5:7e:0d:
        f8:63:de:da:f0:59:2c:dc:3f:b6:c6:4a:9c:98:79:
        6d:21:fa:73:f5:39:bb:6a:86:61:73:d4:43:ae:2d:
        8a:1d:d5:9b:b5:ea:d3:fe:09:70:80:07:85:0f:0f:
        3c:98:1c:1d:48:ed:57:4f:36:f7:f9:21:9f:3b:e5:
        2a:bb:e8:d3:7d:6d:a4:20:e1:4d:cf:2e:21:ec:60:
        00:7c:17:ef:70:2a:4a:30:32:27:52:b2:7d:fb:96:
        7f:03:28:08:25:b3:b5:9d:2b:99:93:8f:57:64:ce:
        c6:21:32:7f:9a:f9:ab:28:08:93:00:69:46:97:c1:
        2f:90:98:a5:4a:1f:b9:84:3c:96:ea:1d:e5:ff:1a:
        c0:9d:e3:61:be:9d:54:04:03:e8:a4:c3:af:bf:c2:
        4a:69:90:d1:6f:a4:fc:46:61:2f:cc:fb:a1:1c:e1:
        1b:12:71:6d:4e:af:f7:54:f4:39:25:d0:9f:b5:64:
        8c:44:4e:43:4a:27:18:ef:54:71:6b:d0:f6:25:ec:
        b7:29:45:8c:8a:69:76:ef:e5:a7:d7:63:25:9f:d4:
        29:08:73
      Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption

```

*Ilustración 20 Captura 1 en modo texto de un certificado digital x509*

```

Signature Value:
1f:ec:36:7b:b7:81:a1:7a:52:d1:ef:7f:fb:83:6d:a3:aa:5c:
11:27:d1:0a:81:2c:30:fe:4b:5e:1d:a8:07:28:ee:5d:9d:0c:
20:b1:d9:f0:d9:a5:5c:9c:21:bd:53:50:aa:ea:02:25:be:72:
e0:72:42:ad:9d:72:dd:8a:cb:56:40:84:4b:94:6c:f1:c5:50:
b6:78:40:6f:85:26:e3:32:5c:56:08:03:28:ec:17:f4:8f:4b:
fa:c9:f1:4a:b3:e5:ad:dd:aa:3f:f3:73:bf:e0:86:e7:fd:cb:
cb:f8:a7:e3:8a:bb:65:cf:46:7c:4c:4a:33:a4:cb:64:0a:a0:
15:86:1a:00:9a:a2:6e:59:42:11:5a:7b:55:62:ad:74:0f:50:
1c:ab:58:69:bc:48:70:84:8d:19:21:73:d2:99:61:31:10:a3:
8a:06:1e:e7:98:6b:79:c0:79:9f:26:c0:d8:94:b9:55:d8:35:
59:d6:3b:00:97:a8:33:f1:fd:4a:82:e3:a0:b9:64:d5:7f:a2:
c0:49:e1:70:2a:29:19:de:a5:65:2f:17:9d:8b:c1:90:26:a9:
28:9a:fc:de:e8:cf:a8:65:78:2b:06:08:7c:4d:2e:13:4e:75:
3a:da:f7:33:6d:59:eb:0c:51:32:3d:fc:b0:0d:ae:50:93:32:
15:d0:49:68:54:18:02:a6:bc:d6:9a:2a:df:ec:d6:79:9e:1e:
ed:15:dc:95:2d:fb:c7:f5:4c:f2:3b:43:71:15:09:60:fc:4a:
03:80:a3:5a:41:30:fb:3a:86:fd:3a:bc:20:8a:1b:40:64:8f:
14:3d:7b:9a:34:52:a0:0b:2b:7e:91:be:2b:30:0d:bd:b9:e1:
f5:89:3e:29:0a:d8:cc:b6:34:08:a8:0c:31:ea:73:ed:32:8b:
92:be:17:5d:c0:99:73:c1:d9:e0:71:e4:15:f0:a0:58:ad:ff:
59:e8:10:55:1f:a6:80:ac:e9:c0:55:fc:cd:1a:d5:7c:fa:6a:
a9:52:ef:84:a2:71:84:70:39:44:fb:ad:a2:6e:b3:e8:03:cf:
6b:6e:fe:36:1f:ac:56:06:8f:7a:b0:4a:ed:57:1d:fe:88:c6:
a0:e0:ea:e4:0b:bc:21:27:ac:95:8f:bb:4d:f4:f2:bd:40:16:
cd:62:bc:d4:2d:ac:1b:51:c4:b7:c6:28:20:a9:d8:f8:3b:d5:
8b:84:8c:c2:90:65:aa:25:48:6a:b1:a2:d5:c0:10:5c:a1:84:
29:38:4f:be:16:fa:de:8f:44:55:ef:bd:4f:0f:1a:f9:cd:34:
fd:c4:8e:31:6c:d4:6c:34:6c:70:d5:0f:6c:13:75:ae:8d:dc:
46:36:af:a9:d8:5b:4c:90
-----BEGIN CERTIFICATE-----
MIIFrzCCA5cCFA+Z0nRShsovWIkNnIw8w+/zPbJ5MA0GCSqGSIb3DQEBCwUAMIGT
MQswCQYDVQQGEwJFUZEPMA0GA1UECwGTFkcnlkMQ8wDQYDVQQHDAZNYWRyaWQx
DDAKBgNVBAoMA1VQTETMBEGA1UECwwKU2Vydmlkb3JlczENMAAGGA1UEAwEUMF1
bDEwMC4GCCqGSIb3DQEJARYhcnF1bC5jYWxkZXJvbi5tb3JhQGFsdW1ub3MudXBt
LmVzMB4XD010MDQyNzIwMjExN10XDTI1MDQyNzIwMjExN1owGZMxCzAJBgNVBAYT
AkVUMQ8wDQYDVQQIDAZNYWRyaWQxZDZANBgNVBAcMBk1hZHJpZDEMMAoGA1UECgwD
VVBNNRMwEQYDVQQLDAPtZXJ2aWRvcnVzMQ8wCwYDVQQDDAR5YXVzMTAwLGYJKoZI
hvcNAQkBFiFyYXVzLnNhbgRlcn9uLm1veWFAWx1bW5vcy51cG0uZXZMwggIiMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQD0bMvy1xwIicFgBk6nZgCXkb03S2YD
aLA/WarCkLrHxDucR79SdovXcJ5736vJB99GfL/qiWPGGQZ3TFNhKIyfbH5PQbeZ
1fMRm7Shm/G4TzpVK3X1fNCgSAJtkN1Vb+K0XSNF50lkDBRhmP283RV+AtERP11
A8YpQtzHT7OI4CbLvrS822bry2GWD1/jE1NQ1jd3nvMPUXY44KgVGLjdW9zA64kFQ
lQIddHPpt1ssHUQvx8Fr801T9DrcSa9eWf5kGSak0Y03A79QvEjoieDWrdS0vo30
m+X1Ky8dJt08KbWddednYJECALGe/AEe+3az0npJn2LLTzzGS7xfanHp9u/NP5R0
nRgSTHw0BtlyrXAE9THEEz6HQZqRL4MwX204KNTxoHnV/V+Dfhj3trwMSzcP7BG
SpyYeW0h+nP10btqhmFz1E0uLYod1Zu16tP+CXcAB4UPDzyYHB1I7VdPNvf5IZ87
5Sg76NN9baQg4U3PLiHsYAB8F+9wKkowMidSsn37ln8DKAgls7WdK5nTj1dkzsYh
Mn+a+asoCJMAaUaXwS+QmKVKH7mEPJbqHeX/GsCd42G+nVQEA+ikw6+/wkppkNFv
pPxGYS/M+6Ec4RsScW10r/du9Dkl0J+1ZIXETkNKJxjvVHFr0PYl7LcPRYyKaXbv
SafXYyWf1CkIcwIDAQABMA0GCSqGSIb3DQEBCwUAA4ICAQAF7DZ7t4GheLLR73/7
g22jqLwR9JEKqSww/kteHagHK05dnQwgsdnw2aVcnCG9U1Cq6gIlvnLgckKtnXLD
istWQIRLlgzxxVC2eEBvhSbjmLxWCAMo7Bf0j0v6yfFKs+Wt3ao/830/4Ibn/cvL
+KfjirtLz0Z8TEozpMtkCqAVhhoAmqJuUIRWntVYq10D1Acq1hpnvEhwhI0ZIXPS
mWExEK0KBh7nmGt5wHmfJsDYLLV2DVZ1jsAl6gz8f1Kgu0guWTVf6LASEfWkikZ
3qVLLxed18GQJqkomvze6M+oZXgrBgh8TS4TTnU62vczbVnrDFEyPfywDa5QkzIV
0EloVBgCprzWmirf7NZ5nh7tFdyVLfvH9Uzy00NxFQlg/EoDgKNaQTD70ob90rWg
ihtAZI8UPXuanFKgCyt+kb4rMA29ueH1iT4pCtjMtjQIqAwX6nPtMouSvhdwJlZ
wdngceQV8KBYrf9Z6BBVH6aArOnAVfzNGtV8+mqpUu+EonGECdLE+62ibrPoA89r
bv42H6xWBo96sErtVx3+iMag40rkC7whJ6yVj7tN9PK9QBbNYrzULawbUcS3xiGg
qdj409WLIhZCkGWqJUHQsaLVwBBcoYQpOE++Fvrej0RV771PDxr5zTT9xI4xbNRs
NGxw1Q9sE3WujdxGNq+p2FtMkA==
-----END CERTIFICATE-----

```

Ilustración 21 Captura 2 en modo texto de un certificado digital x509

Pregunta 13. ¿Para qué vale la extensión subjectAltName? ¿Por qué crees que es importante para TLS?

Subject Alternative Name es un nombre alternativo a X.500 para identificar a la entidad propietaria(según apuntes de la asignatura), que se utiliza para especificar valores alternativos de sujetos en el propio certificado e incluso sirve para indicar el valor de CN (nombre común).

Esta extensión es importante para TLS porque se utiliza para el proceso de validación del certificado.

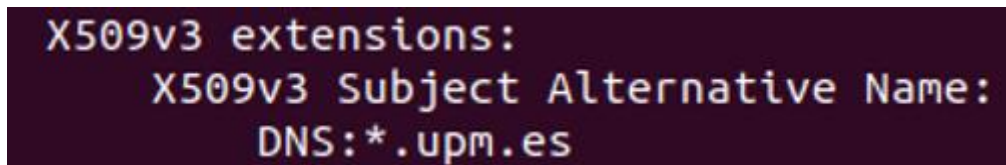


Ilustración 22 Captura con la extensión agregada al certificado X509

Pregunta 14. ¿Qué ha cambiado respecto al certificado anterior?

```
user@user-virtual-machine:~$ openssl x509 -req -days 365 -in petition.csr -signkey clave_privada_CA.pem -extfile ficheroExtension.txt -out certificadoExtension.cert
Certificate request self-signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
user@user-virtual-machine:~$ openssl x509 -in certificado
certificadoCreado.crt      certificadoExtension.cert
user@user-virtual-machine:~$ openssl x509 -in certificadoExtension.cert -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            33:f8:1b:47:bb:b9:f8:2a:18:15:0f:32:b8:e6:dc:c1:04:0a:29:64
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
        Validity
            Not Before: Apr 28 17:25:41 2024 GMT
            Not After : Apr 28 17:25:41 2025 GMT
        Subject: C = ES, ST = Madrid, L = Madrid, O = UPM, OU = Servidores, CN = Raul, emailAddress = raul.calderon.moya@alumnos.upm.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
```

Ilustración 23 Captura 1 certificado X509v3

```

Modulus:
00:db:32:fc:b5:c7:02:22:70:58:01:93:a9:d9:80:
25:e4:6f:4d:d2:67:76:03:6a:50:3f:59:aa:c2:92:
5a:c7:c4:35:1c:47:bf:52:76:8b:d7:70:9e:7b:df:
ab:c9:07:df:46:7e:5f:ea:89:63:c6:81:06:77:4d:
f3:61:28:8c:9f:06:1e:4f:41:b7:99:d5:f3:11:9b:
b4:a1:9b:f1:b8:4f:3a:55:2b:75:f5:7c:d0:a0:48:
02:6d:90:dd:55:6f:e2:b4:5d:23:45:e4:e9:64:0c:
14:61:1e:63:f6:f3:74:55:f8:0b:44:44:f2:35:03:
c6:29:42:dc:c7:ec:e2:38:09:b2:ef:ad:2f:36:d9:
ba:f2:d8:65:83:d7:f8:c4:d4:d4:35:8d:dd:e7:bc:
c3:d4:5d:8e:38:2a:05:46:2e:37:56:f7:30:3a:e2:
41:50:95:02:1d:74:73:cf:b7:5b:2c:1d:44:2f:c7:
c1:6b:f3:4d:53:f4:3a:dc:49:af:5e:59:fe:64:19:
26:a4:d1:83:b7:03:bf:50:bc:48:e8:89:e0:d6:ad:
d4:b4:be:8d:f4:9b:e5:f5:2b:2f:1d:26:d3:bc:29:
b5:9d:75:e7:67:60:91:1c:00:b1:9e:fc:01:1e:fb:
76:b3:3a:7a:49:9f:62:cb:4f:3c:c6:4b:bc:5f:6a:
71:e9:f6:ef:cd:3f:94:4e:9d:18:12:4c:75:b4:06:
d9:72:ad:70:04:f5:38:44:13:3e:87:41:06:6a:46:
5e:0c:c1:7d:b4:e0:a3:53:c6:81:e7:57:f5:7e:0d:
f8:63:de:da:f0:59:2c:dc:3f:b6:c6:4a:9c:98:79:
6d:21:fa:73:f5:39:bb:6a:86:61:73:d4:43:ae:2d:
8a:1d:d5:9b:b5:ea:d3:fe:09:70:80:07:85:0f:0f:
3c:98:1c:1d:48:ed:57:4f:36:f7:f9:21:9f:3b:e5:
2a:bb:e8:d3:7d:6d:a4:20:e1:4d:cf:2e:21:ec:60:
00:7c:17:ef:70:2a:4a:30:32:27:52:b2:7d:fb:96:
7f:03:28:08:25:b3:b5:9d:2b:99:93:8f:57:64:ce:
c6:21:32:7f:9a:f9:ab:28:08:93:00:69:46:97:c1:
2f:90:98:a5:4a:1f:b9:84:3c:96:ea:1d:e5:ff:1a:
c0:9d:e3:61:be:9d:54:04:03:e8:a4:c3:af:bf:c2:
4a:69:90:d1:6f:a4:fc:46:61:2f:cc:fb:a1:1c:e1:
1b:12:71:6d:4e:af:f7:54:f4:39:25:d0:9f:b5:64:
8c:44:4e:43:4a:27:18:ef:54:71:6b:d0:f6:25:ec:
b7:29:45:8c:8a:69:76:ef:e5:a7:d7:63:25:9f:d4:
29:08:73
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:*.upm.es
X509v3 Subject Key Identifier:
90:AF:3E:DB:AE:85:CE:17:30:A1:AD:C5:47:63:5A:48:AE:C1:85:E2
Signature Algorithm: sha256WithRSAEncryption

```

Ilustración 24 Captura 2 certificado X509v3

Como se aprecia en la captura, los cambios los encontramos en la parte de versión que, en este caso, pasa a tener versión 3 en lugar de versión 1, junto con el valor de la extensión agregada que figura dentro del campo creado “X509v3 Extensions” de las capturas previas.

### 3. Conexiones basadas en TLS

Pregunta 15. En la ejecución que has realizado, ¿Qué conjunto de algoritmos criptográficos se han elegido para la sesión?

#### Creación Cliente y conexión TLS con el servidor

```

user@user-virtual-machine:~$ sudo adduser cliente
[sudo] password for user:
Adding user `cliente' ...
Adding new group `cliente' (1001) ...
Adding new user `cliente' (1001) with group `cliente' ...
Creating home directory `/home/cliente' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for cliente
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
user@user-virtual-machine:~$ su - cliente
Password:
cliente@user-virtual-machine:~$ ls

```

Ilustración 25 Captura creación usuario cliente



```

cliente@user-virtual-machine:~$ openssl genrsa -out clave_privada.pem 4096
cliente@user-virtual-machine:~$ openssl rsa -in clave_privada.pem -pubout -out clave_publica.pem
writing RSA key
cliente@user-virtual-machine:~$ ls
clave_privada.pem  clave_publica.pem

```

*Ilustración 26 Captura creación de clave privada y pública para el usuario cliente*

```

cliente@user-virtual-machine:~$ openssl req -new -key clave_privada.pem -out peticionCliente.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:MADRID
Locality Name (eg, city) []:MADRID
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPM
Organizational Unit Name (eg, section) []:SEGURIDAD
Common Name (e.g. server FQDN or YOUR name) []:CLIENTE
Email Address []:CLIENTE

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
cliente@user-virtual-machine:~$ ls
clave_privada.pem  clave_publica.pem  peticionCliente.csr
cliente@user-virtual-machine:~$ openssl x509 -req -days 365 -in peticionCliente.csr -signkey cla
ve_privada.pem -out certificadoCliente.cert
Certificate request self-signature ok
subject=C = ES, ST = MADRID, L = MADRID, O = UPM, OU = SEGURIDAD, CN = CLIENTE, emailAddress = C
LIENTE

```

*Ilustración 27 Captura creación petición de certificación para el usuario cliente*

```

cliente@user-virtual-machine:~$ openssl s_client -connect 127.0.0.1:4443 -cert certificadoClient
e.cert -key clave_privada.pem -msg -status -sess_out ficheroSesion | cat > ficheroMensajes
Can't use SSL_get_servername
depth=0 C = ES, ST = MADRID, L = MADRID, O = UPM, OU = SEGURIDAD, CN = RAUL, emailAddress = Serv
idor
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = ES, ST = MADRID, L = MADRID, O = UPM, OU = SEGURIDAD, CN = RAUL, emailAddress = Serv
idor
verify return:1
Hola soy cliente

```

*Ilustración 28 Captura para establecimiento de conexión con un servidor*

```

cliente@user-virtual-machine:~$ ls
certificadoCliente.cert  clave_privada.pem  clave_publica.pem  ficheroMensajes  ficheroSesion p
eticionCliente.csr

```

*Ilustración 29 Captura con listado de archivos generados en la máquina cliente*

Ahora si ejecutamos el comando `cat ficheroMensajes`, vemos lo siguiente:

```

SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384

```

*Ilustración 30 Captura con algoritmos de cifrado en la sesión SSL*

```

---
read R BLOCK
>>> TLS 1.2, RecordHeader [length 0005]
    17 03 03 00 22
>>> TLS 1.2, InnerContent [length 0001]
    17
<<< TLS 1.2, RecordHeader [length 0005]
    17 03 03 00 33
<<< TLS 1.3, InnerContent [length 0001]
    17
Recibido cliente, soy el servidor

```

*Ilustración 31 Captura interacción durante la conexión entre cliente y servidor*

```

cliente@user-virtual-machine:~$ cat ficheroMensajes
CONNECTED(00000003)
>>> TLS 1.0, RecordHeader [length 0005]
    16 03 01 01 29
>>> TLS 1.3, Handshake [length 0129], ClientHello
    01 00 01 25 03 03 01 64 d7 d8 02 6a e2 76 ba 5f
    66 e7 74 82 dd 70 fb 42 62 6f d5 d2 3f 16 89 cf
    2d c7 9b af 21 fd 20 07 b0 eb 39 fc 6a 04 41 11
    fd 5a 83 ca f5 de b4 7f 27 1c db a0 64 ce 15 4b
    5f 4b 93 83 c7 cb 52 00 3e 13 02 13 03 13 01 c0
    2c c0 30 00 9f cc a9 cc a8 cc aa c0 2b c0 2f 00
    9e c0 24 c0 28 00 6b c0 23 c0 27 00 67 c0 0a c0
    14 00 39 c0 09 c0 13 00 33 00 9d 00 9c 00 3d 00
    3c 00 35 00 2f 00 ff 01 00 00 9e 00 0b 00 04 03
    00 01 02 00 0a 00 16 00 14 00 1d 00 17 00 1e 00
    19 00 18 01 00 01 01 01 02 01 03 01 04 00 23 00
    00 00 05 00 05 01 00 00 00 00 00 16 00 00 00 17
    00 00 00 0d 00 2a 00 28 04 03 05 03 06 03 08 07
    08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01
    05 01 06 01 03 03 03 01 03 02 04 02 05 02 06 02
    00 2b 00 05 04 03 04 03 03 00 2d 00 02 01 01 00
    33 00 26 00 24 00 1d 00 20 2d f0 88 19 95 06 88
    44 44 1c a3 a8 6a e0 46 07 19 5b ea c5 9d d3 cf
    31 c5 8c 3e 70 f1 03 3e 77
<<< TLS 1.2, RecordHeader [length 0005]
    16 03 03 00 7a
<<< TLS 1.3, Handshake [length 007a], ServerHello

```

*Ilustración 32 Captura 1 de ficheroMensajes*

```

Certificate chain
0 s:C = ES, ST = MADRID, L = MADRID, O = UPM, OU = SEGURIDAD, CN = RAUL, emailAddress = Servidor
i:C = ES, ST = MADRID, L = MADRID, O = UPM, OU = SEGURIDAD, CN = RAUL, emailAddress = Servidor
a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
v:NotBefore: Apr 30 14:22:38 2024 GMT; NotAfter: Apr 30 14:22:38 2025 GMT

```

*Ilustración 33 Captura 2 de ficheroMensajes*

Por otro lado, si ejecutamos `cat ficheroSesion`, vemos lo siguiente:

```

cliente@user-virtual-machine:~$ cat ficheroSesion
-----BEGIN SSL SESSION PARAMETERS-----
MIIG4AIBAQAICAwQEAMCBCC89zj+2BRfc+LxwTMrU5MRAlIdJyiWlXRujSYbXVqH
DgQw+3MoEP4rOkZu9lCLuLIA180SvGdvTFcoTQEADtSPV3oKqtGmFwyzNXxWE0
1DQvoQYCBGYw/4q1BAIHCCHjggv9MIIEFTCAAECEFHLLw05ovt+h3DueQ4uk/Rwz/
eRVMDMA0GCSqGSIb3DQEBCwUAMHkCzAABGNVBAYTAkVtM08wDQYDVQQIDAZNQURS
SUQXDzANBgNVBACMBk1BRFJJRDDEMMAoGA1UECgwDVBNMIRIEAYDQQLDALTRudV
UkLEQUQxDTALBgNBAMBMFBjBVUwXFAZABGkqhkiG9w0BCQEWCENlcnZpZG9yYMB4X
DTI0MDQzMDME0MjJzOfoXDTI1MDQzMDME0MjJzOfoWetELMAKGA1UEBmRCMCRVMDZAN
BgNVBAGMBk1BRFJJRDDEMMAoGA1UEBmVzTUFEUkLEMQwwXG9yDQYDVQQIDANVb0E0eJjAQ
BgNVBAsCMCVNFR1VSSURBRDENMAsGA1UEAwwEUKFvTDXEAMBUGCSqGSIb3DQEJARYI
U2VydmlkY3IwggIiMA0GCSqGSIb3DQEBAQUAA4ICDABBggIKAoICAQDGzdvycfuI
JvYwMianVmz+FtgCxxuU3/iLEG68Y10833Ee/ksNBCrzGp0jH5+mYOX+tDEQPXwka
ko4LDRqpS55HkL7i1L5CA+L5NK/mgs+wSiX8mUoqKA3k5h06dQYJcF/nmWq+0Zn
XosNNmpEK9ZKZS80VCSyUA9C4wWcrZ90yWwVdloyIftTAMAvJGgunfB2RM/VAYPU
9J/DNYoNaP047/LY9+cnopDi4oerEeUdhH50cgYBPFFjlxLwmftt9+WmRPz/wtI8h
eM3INHqNuA4QJhE/EwDexN4n04r4jQ++jyfxxA7HtavNhFftDnVMnqpo30XSnuJ
Cy3cS15UzPnn4g6jxMgoUKEkk1du8tHyA0Dco20K0dITgYJ+KvNPENd8WuH7Nq7P
0h9jzt1puG679qW2G0vYyuEmEZFD0facuTH/P5I3LZXsvpxmJn/Vo6kh8Eo1Lw5Q
vEyZ506kGHVSougR877pYz+2z6VARD//vstItqpCKdgd/nUoCQ4iGAd60aoXkMb
2ZR9fBHII8xvD7YArg+pi98Pxok26JapK3m15u4tLUe7ntK8+5mQnn5MKz4j/de
yATA6qZzeBoPomsWH20+Dm+DSQhR4vPuPuqSKTwzjZT5mLakKA7FEeKysveZJ1HF
ebiA6/3a+ow2Clxo+lyWkqVX6ptTga//JQIDAQABMA0GCSqGSIb3DQEBCwUAA4IC
AQAAIohh85Jyia14vrkLta4LpB8vI1igpOHLHkYJLY/DbrMZAemj3BiddROM+KM
3cN4lkl3ym7tLkHA78mTL9ik3xzIaga+nbSsQ+PNWt4TEjKJMQfLLfICMqf7qo2P+
jLjRwXKGAyfqVZQByX84fORLacInPV7a0n064J20TtHcBDJwepB8VeQvSfn0SRZIE
H9LCXBpnlj+6jEcfMVqj4bmUQaitVIKUETWPLXntfWUy2qgSubrO86oEno4LBphXK
7SvF7+mISVQeDARwVBDFDK5GyXIFto0AchyFRx7zSeCn+7Rku61AV7PF8IRVDZ8v
Ndt0g/Y88vbJ194ydhEduETV1lcAfHLu4yvkI/0NVOK2YD/cv4RwZCC6m0GZWRpZ
Ed3Jlzh0/7ArKRD2XJdyUqLrnmJrnoMDnOgnY0R57Ard0C6+IuGw/qqs6y6dglGv3
yaTknpfTebaVvXUYD5bh5aX5cr2zm8W6N0YLnViOfOfoQeAlFRKoyE/2rjks+Xdo+
4otgG/n14DIhw/Qm7mzhFbaq2NZ1F08d0WEJk4LHMVC31/KUZbfmImV5N0jKRS9W
Q3CzmMx0RJwoM165DbGNjBo14Wacywfm9yZuR01wrXQpCqqqFYBQznLgYTbwf8v
HXpU6VVK5ELP54+00rx03Aw/In5vd3SngJDRNT+0DpjJcKAQCBACLAIBEQeAgEaTc
IKqB0WSB0A47XfzB7vewIi5sLzTTB5HOFLuMljJqfud9m31hGstcQSLBS5GLPtAd
p3U2zmKzxfZp/8No6JmZa3mYeLMj317N/QAIGPtoojXIrXDHsIb00sciJrQqUj3X
wBITmZAYsaUhxbst1PEfyKts+4DHGI4AQsf12oKrpFHfU9ZrNct4AYW2geBnZ+k5
s/DHAARFXm+WZK94JKJMVNT2grHgd3iGoStnoqMLBHFD4fZL65UYOfvzf7tm04Ql
to5bv1qLRQfORebI72hdS0iD7nnk12+uBgIEAQGusbMDAgEd
-----END SSL SESSION PARAMETERS-----

```

### Ilustración 34 Captura Contenido ficheroSesion

## Creación Servidor y conexión TLS con el cliente

```
user@user-virtual-machine:~$ sudo adduser servidor
Adding user `servidor' ...
Adding new group `servidor' (1002) ...
Adding new user `servidor' (1002) with group `servidor' ...
Creating home directory `/home/servidor' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for servidor
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
user@user-virtual-machine:~$ su - servidor
Password:
```

*Ilustración 35 Captura creación del usuario servidor*

```
servidor@user-virtual-machine:~$ openssl genrsa -out clave_privada.pem 4096
```

*Ilustración 36 Captura creación clave secreta para el usuario servidor*

```
servidor@user-virtual-machine:~$ openssl rsa -in clave_privada.pem -pubout -out clave_publica.pem
writing RSA key
servidor@user-virtual-machine:~$ ls
clave_privada.pem  clave_publica.pem
```

*Ilustración 37 Captura creación de la clave pública a partir de la privada en el usuario servidor*

*Ilustración 38 Creación de petición de certificación para el usuario servidor y creación de certificado X509*

*Ilustración 39 Captura de lanzamiento del servidor e interacción con el cliente por parte del usuario servidor*

### Pregunta 16. ¿Qué es un Session-ID? ¿Qué es una master Key?

El valor de Session-ID lo envía el cliente al servidor y éste consulta a ver si conoce dicho valor y en caso de tener dicho valor almacenado vuelve a establecer la sesión con el cliente. Con lo cual, el valor de Session-ID permite en caso de perder la conexión que se pueda reanudar de manera rápida sin necesidad de volver a repetir el protocolo Handshake de nuevo.

Por otro lado, una Master key es una clave secreta utilizada en TLS utilizada para realizar cifrado y descifrado de los datos que se transmiten cliente y servidor durante una sesión TLS. La clave Master Key se acuerda entre cliente y servidor durante el protocolo Handshake.

**Pregunta 17.** ¿Se ha elegido algún algoritmo de compresión? ¿Dónde se incluye la compresión dentro del procesamiento de un paquete por parte del TLS? Pista: hay una diapositiva en la presentación Introducción a TLS de Moodle dónde se indica cómo se transforma el paquete dentro de TLS.

No se ha elegido ningún algoritmo de compresión. Todo lo relacionado con la parte de compresión va en la parte de Record Protocol.

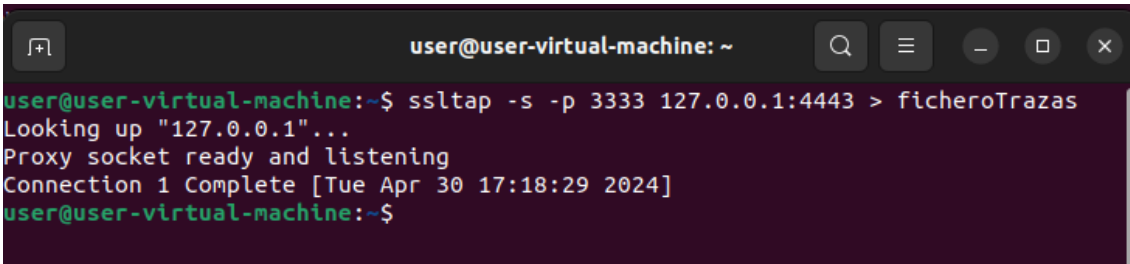
**Pregunta 18.** ¿Qué material criptográfico temporal necesita cada una de las entidades para establecer una sesión? Pista: hay una diapositiva donde aparece.

En el lado del cliente, debe contar con su clave privada y clave pública, junto con la clave pública de la otra entidad (el servidor), RSs o número aleatorio generado por el servidor, valor de Pre-Master-Secret que se envía según los apuntes cifrado con la clave pública del servidor y; por último, el valor Master-Secret.

En el lado del servidor, debe contar con su clave privada y clave pública, junto con la clave pública de la otra entidad (el cliente), RSc o número aleatorio generado por el cliente, valor de Pre-Master-Secret que se envía según los apuntes cifrado con la clave pública del servidor y; por último, el valor Master-Secret.

## Monitorización con SSLTAP

Usuario Root

A screenshot of a terminal window with a dark background. The window title is 'user@user-virtual-machine: ~'. The terminal shows the following commands and output: 

```
user@user-virtual-machine:~$ ssltap -s -p 3333 127.0.0.1:4443 > ficheroTrazas
Looking up "127.0.0.1"...
Proxy socket ready and listening
Connection 1 Complete [Tue Apr 30 17:18:29 2024]
user@user-virtual-machine:~$
```

*Ilustración 40 Captura de la terminal del lado del usuario root*



```

servidor@server-virtual-machine:~$ openssl s_server -accept 4443 -cert certificadoServidor.cert -key clave_privada.pem
Using default temp DH parameters
ACCEPT
-----BEGIN SSL SESSION PARAMETERS-----
MIICAgIBADBAQgEYELINjbm9v/F8lpghBSc0ZxOmdyLWUwLTd4cGkiZWls
DDBKRXR0K6so7TlBRVU/kn0kqf/FcmhdjDE4vtLSmwpmwyIPecuqqltHmXii
vsqhBgIEZjElBKTEAgiCIKCBAQAQAAsAA9VCXBVDWakZzAwTBHQ==
-----END SSL SESSION PARAMETERS-----
Shared cipher: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDH:ECDHE-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDH-ECDSA-CHACHA20-POLY1305
:ECDH-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA384:DHE-RSA-AES256-SHA384:ECDH-RSA-AES128-SHA:ECDH-RSA-AES128-SHA:ECDSA-AES256-GCM-SHA384:AES256-GCM-SHA384:AES256-SHA:ECDSA-AES256-SHA:ECDSA-AES128-SHA:ECDSA-AES128-SHA:ECDSA-AES128-SHA-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SMASH12:Ed25519:Ed448:RSA-PS+SHA256:RSA-PS+SHA384:RSA-PS+SMASH12:RSA-PS+SHA256:RSA-PS+SHA384:RSA-PS+SMASH12:RSA+SHA256:RSA+SHA384:RSA+SMASH12:ECDSA+
+SHA224:RSA+SHA224:DSA+SHA224:DSA+SHA256:DSA+SHA384:DSA+SMASH12
Secure Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SMASH12:Ed25519:Ed448:RSA-PS+SHA256:RSA-PS+SHA384:RSA-PS+SMASH12:RSA-PS+SHA256:RSA-PS+SHA384:RSA-PS+SMASH12:RSA+SHA256:RSA+SHA384:RSA+SMASH12
2:ECDSA+SHA224:RSA+SHA224
Supported groups: x25519:secp256r1:x448:secp252r1:secp384r1:fFdhE2048:fFdhE3072:fFdhE4096:fFdhE6144:fFdhE8192
Shared groups: x25519:secp256r1:x448:secp252r1:secp384r1:fFdhE2048:fFdhE3072:fFdhE4096:fFdhE6144:fFdhE8192
CIPHER is TLS_AES_256_GCM_SHA384
Secure Renegotiation Is supported
HOLA SOY CLIENTE DE LA PARTE SLLATP

```

## Cliente

```

root@kali:~# openssl s_client -connect 127.0.0.1:3333 -cert certificadoCliente.cert -key clave_privada.pem -msg -status -sess_out ficheroSesion | cat > ficheroMensajes
Can't use SSL get servername
depth=0 C = ES, ST = MADRID, L = MADRID, O = UPW, OU = SEGURIDAD, CN = RAUL, emailAddress = Servidor
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = ES, ST = MADRID, L = MADRID, O = UPW, OU = SEGURIDAD, CN = RAUL, emailAddress = Servidor
verify return:1
HOLA SOY CLIENTE DE LA PARTE SSLTAP

```

Pregunta 19. ¿Cuántos conjuntos de algoritmos criptográficos (suites) se han intercambiado para poder elegir uno?

*Ilustración 43 Captura de suites de cifrado intercambiados*

RAÚL CALDERÓN MOYA

Pregunta 20. ¿Qué tipos de registros (SSLRecord) se observan?

Hay tres tipos de ellos que son Handshake, change\_cipher\_spec y application\_data.

```
SSLRecord { [Tue Apr 30 17:17:00 2024]
  type    = 20 (change_cipher_spec)
  version = { 3,3 }
  length  = 1 (0x1)
}
(2217 bytes of 23, with 2056 left over)
SSLRecord { [Tue Apr 30 17:17:00 2024]
  type    = 23 (application_data)
  version = { 3,3 }
  length  = 23 (0x17)
  < encrypted >
}
```

*Ilustración 44 Captura 1 de los registros SSL Record*

```

SSLRecord { [Tue Apr 30 17:17:00 2024]
  type      = 22 (handshake)
  version   = { 3, 3 }
  length    = 122 (0x7a)
  handshake {
    type     = 2 (server_hello)
    length   = 118 (0x000076)
    ServerHello {
      server_version = {3, 3}
      random         = {...}
      session ID    = {
        length = 32
        contents = {...}
      }
      cipher_suite = (0x1302) ?????/????????/????????/???
      compression method = (00) NULL
      extensions[46] = {
        extension type 43, length [2] = {
          0: 03 04
          }
        extension type 51, length [36] = {
          0: 00 1d 00 20 e9 f0 ae b8 28 5f 1f ae 2f 71 36 83
          10: e8 d6 d2 a7 4a 48 1d 47 a9 55 8d 27 f7 17 fd 21
          20: 60 91 24 20
          }
        }
      }
    }
  }
}

```

*Ilustración 45 Captura 2 de los registros SSL Record*

## PARTE 2 Práctica 3

## 1. Escenario 0

Pregunta 21. ¿Qué reglas se encuentran actualmente definidas?

```
user@user-virtual-machine:~$ sudo sysctl -w net.ipv4.conf.all.route_localnet=1
[sudo] password for user:
net.ipv4.conf.all.route_localnet = 1
user@user-virtual-machine:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

*Ilustración 46 Captura con el comando de sudo iptables -L y muestra de iptables*

Como se aprecia en la captura, no hay reglas definidas son INPUT, FORWARD Y OUTPUT. Según se aprecia están definidas con política “ACCEPT”, lo cual supone que se aceptará todo el tráfico excepto que se modifiquen dichas reglas.

Pregunta 22. Vuelve a comprobar el estado de las reglas con el comando del paso 1. Comenta los cambios más importantes con respecto a lo obtenido en la pregunta anterior.

```

user@user-virtual-machine:~$ sudo ufw enable
Firewall is active and enabled on system startup
user@user-virtual-machine:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ufw-before-logging-input  all  --  anywhere              anywhere
ufw-before-input          all  --  anywhere              anywhere
ufw-after-input           all  --  anywhere              anywhere
ufw-after-logging-input   all  --  anywhere              anywhere
ufw-reject-input          all  --  anywhere              anywhere
ufw-track-input           all  --  anywhere              anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination
ufw-before-logging-forward all  --  anywhere              anywhere
ufw-before-forward        all  --  anywhere              anywhere
ufw-after-forward         all  --  anywhere              anywhere
ufw-after-logging-forward all  --  anywhere              anywhere
ufw-reject-forward        all  --  anywhere              anywhere
ufw-track-forward         all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ufw-before-logging-output all  --  anywhere              anywhere
ufw-before-output         all  --  anywhere              anywhere
ufw-after-output          all  --  anywhere              anywhere
ufw-after-logging-output  all  --  anywhere              anywhere
ufw-reject-output         all  --  anywhere              anywhere
ufw-track-output          all  --  anywhere              anywhere

Chain ufw-after-forward (1 references)
target     prot opt source                destination

```

*Ilustración 47 Captura de activación del servicio ufw y muestra de iptables*

En este caso, sí hay reglas definidas para las situaciones de before, after, reject y track. Un cambio significativo es que en lugar de ser INPUT, OUTPUT o FORWARD ahora figura DROP, lo que supone que el tráfico será rechazado excepto en los casos en los que se verifiquen las reglas.

### Prueba de conexión con PING entre máquina anfitriona y máquina virtual:

|   |   |
|---|---|
| <pre> user@user-virtual-machine:~\$ ifconfig ens33: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt;  mtu 1500     inet 192.168.139.128 netmask 255.255.255.0  broadcast 192.168.139.255     inet6 fe80::a21c:3a4:58cf:a784 prefixlen 64  scopeid 0x20&lt;link&gt;     ether 08:0c:29:d9:7c:f8 txqueuelen 1000 (Ethernet)     RX packets 30180 bytes 35093174 (35.0 MB)     RX errors 0 dropped 0 overruns 0 frame 0     TX packets 12277 bytes 1205203 (1.2 MB)     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  lo: flags=73&lt;UP,LOOPBACK,RUNNING&gt;  mtu 65536     inet 127.0.0.1 netmask 255.0.0.0     inet6 ::1 prefixlen 128  scopeid 0x10&lt;host&gt;     loop txqueuelen 1000 (Local Loopback)     RX packets 715 bytes 92639 (92.6 KB)     RX errors 0 dropped 0 overruns 0 frame 0     TX packets 715 bytes 92639 (92.6 KB)     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 </pre> | <pre> PS C:\Users\Raúl_PC&gt; ping 192.168.139.128  Haciendo ping a 192.168.139.128 con 32 bytes de datos: Respuesta desde 192.168.139.128: bytes=32 tiempo&lt;1m TTL=64 Respuesta desde 192.168.139.128: bytes=32 tiempo&lt;1m TTL=64 Respuesta desde 192.168.139.128: bytes=32 tiempo&lt;1m TTL=64 Respuesta desde 192.168.139.128: bytes=32 tiempo&lt;1m TTL=64  Estadísticas de ping para 192.168.139.128:     Paquetes: enviados = 4, recibidos = 4, perdidos = 0               (0% perdidos),     Tiempos aproximados de ida y vuelta en milisegundos:         Mínimo = 0ms, Máximo = 0ms, Media = 0ms PS C:\Users\Raúl_PC&gt; </pre> |
|---|---|

*Ilustración 48 Captura con ifconfig desde máquina virtual y ping desde la máquina anfitriona*

Como se puede apreciar sí hay conexión entre ambas máquinas al no haber pérdidas de paquetes (0% perdidos)

## 2. Escenario 1: Gestión de tráfico a un puerto específico

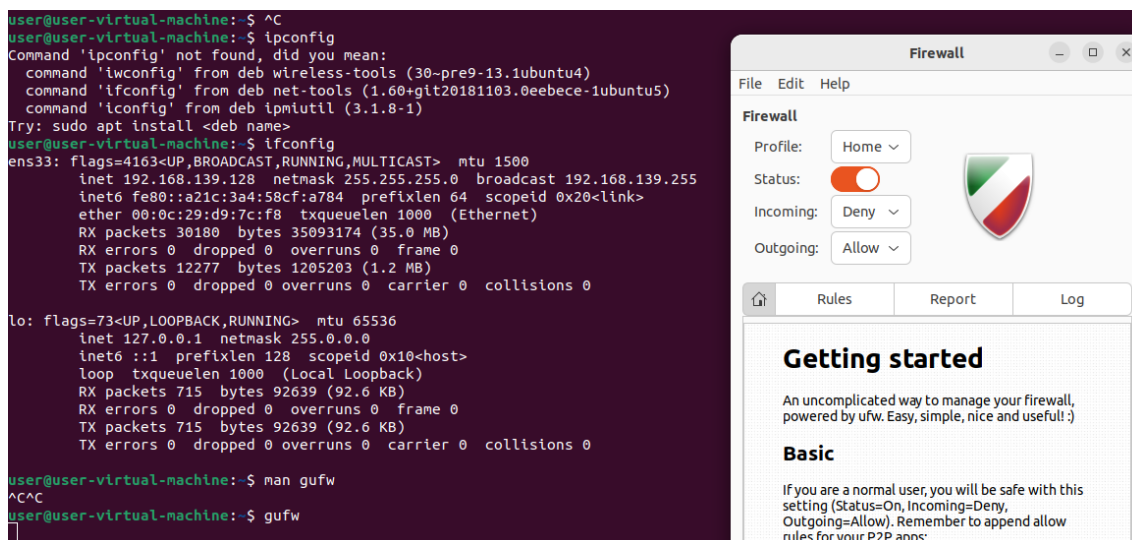
Pregunta 23. Comprueba si es posible realizar una conexión SSH desde la máquina anfitrión a la máquina virtual y comenta el resultado.

```
PS C:\Users\Raúl_PC> ssh user@192.168.139.128
ssh: connect to host 192.168.139.128 port 22: Connection timed out
PS C:\Users\Raúl_PC> |
```

*Ilustración 49 Captura comando ssh desde máquina anfitriona*

En este punto de la práctica, no se puede realizar la conexión SSH ya que se debe habilitar el puerto de TCP con valor 22 en la máquina virtual para que permita las conexiones entrantes, de ahí que no nos deje porque en este momento este servicio se encuentra desactivado.

Pregunta 24. Añade la regla necesaria, utilizando para ello la herramienta GFW, para permitir las conexiones entrantes al servicio SSH desde cualquier dirección de internet. Realiza ahora la prueba de conexión desde la máquina anfitrión e incluye una captura de la regla creada y de su funcionamiento exitoso.



*Ilustración 50 Captura con Interfaz gráfica GFW*

En un primer momento, no hay reglas definidas, pero se agrega la del puerto TCP/22. Esta es la opción por comandos que se hace por UFW, pero hay otra opción que se va a mostrar en breve usando `gufw` o hacerlo con la interfaz gráfica.

```

user@user-virtual-machine:~$ sudo ufw status
[sudo] password for user:
Status: active
user@user-virtual-machine:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
user@user-virtual-machine:~$ sudo ufw enable
Firewall is active and enabled on system startup
user@user-virtual-machine:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

```

Ilustración 51 Versión con comandos para conexión TCP por el puerto 22

Ahora se muestra la forma gráfica de hacerlo con gufw:

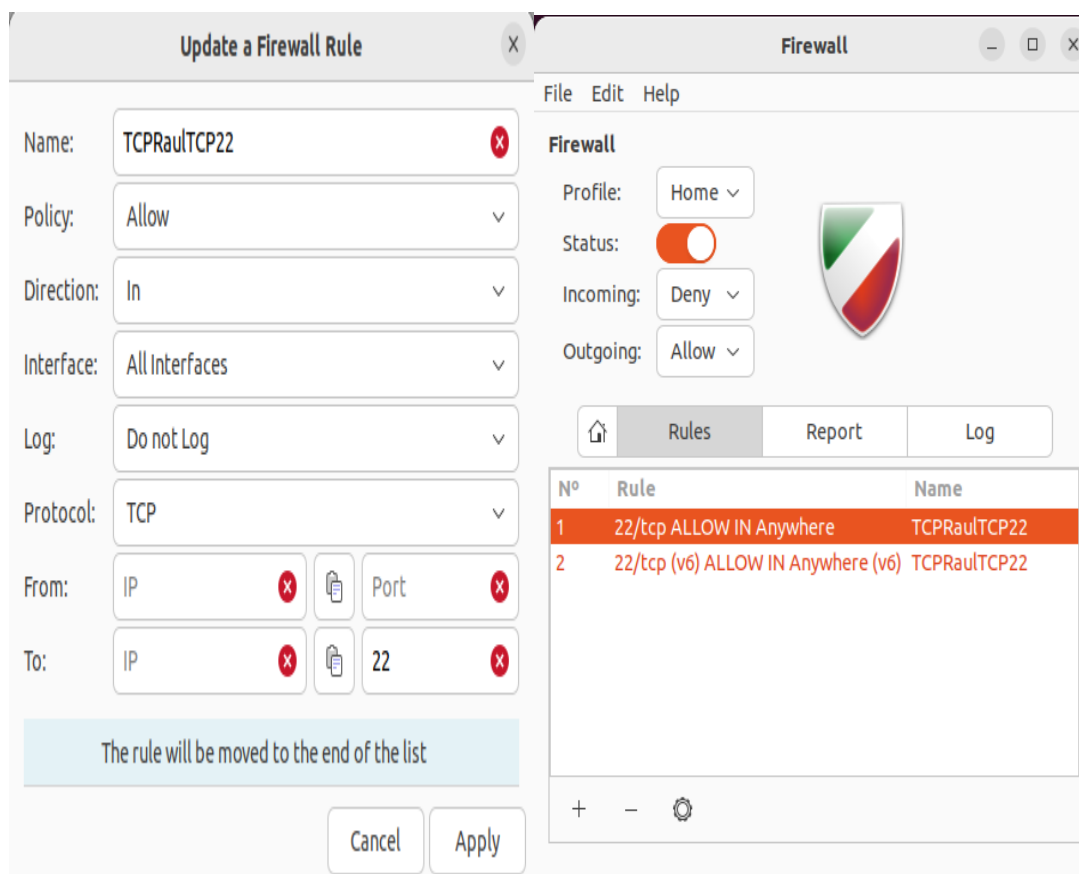


Ilustración 52 Versión con interfaz gráfica GFW para conexión TCP por el puerto 22

Como vemos, según se dice en el enunciado deben permitirse “las conexiones entrantes al servicio SSH desde cualquier dirección de internet”, esto se traduce en poner Direction: In en la GUI de GFW de la máquina virtual, además al ser desde cualquier dirección de Internet no se especifica la IP y por último el puerto debe ser el puerto 22 para que así se pueda completar con éxito el SSH. Tanto si lo hacemos por comandos como de esta última forma el SSH se completa correctamente:



```

PS C:\Users\Raúl_PC> ssh user@192.168.139.128
user@192.168.139.128's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Tue Apr 30 19:11:59 2024 from 192.168.139.1
user@user-virtual-machine:~$

```

Ilustración 53 Conexión SSH correcta desde máquina anfitriona

Pregunta 25. Añade ahora la regla necesaria, utilizando para ello la herramienta GFW, para denegar las conexiones entrantes al servicio SSH únicamente desde la IP de la máquina anfitrión. Realiza ahora la prueba de conexión desde la máquina anfitrión e incluye una captura de la regla creada, demostrando que se ha denegado la conexión a esa IP.

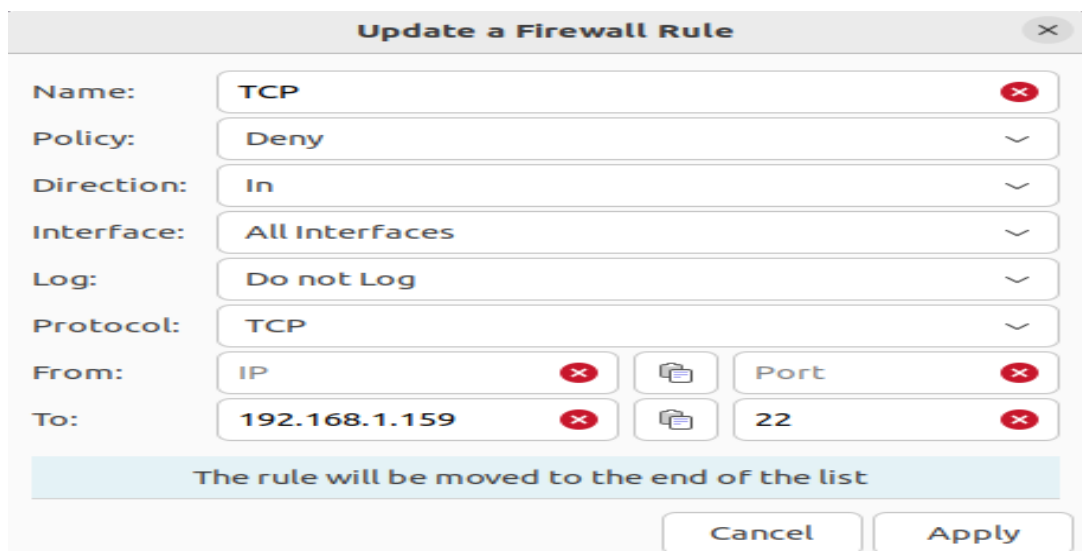


Ilustración 54 Regla definida para denegar acceso desde máquina anfitriona

```

PS C:\Users\Raúl_PC> ssh user@192.168.139.128
ssh: connect to host 192.168.139.128 port 22: Connection timed out
PS C:\Users\Raúl_PC>

```

Ilustración 55 Conexión SSH desde máquina anfitriona

Tal y como se especifica en este escenario, el comando ssh no se puede completar.

### 3. Escenario 2: Redirección de tráfico entre interfaces

Pregunta 26. Añade las reglas necesarias para permitir las conexiones entrantes al servidor web (80/TCP) desde cualquier dirección de internet, redirigiendo SOLAMENTE el tráfico HTTP desde la interfaz ens33 hacia la interfaz de loopback. Realiza una prueba de conexión desde el navegador web de la máquina anfitrión e incluye una captura de la regla creada y de su funcionamiento exitoso.

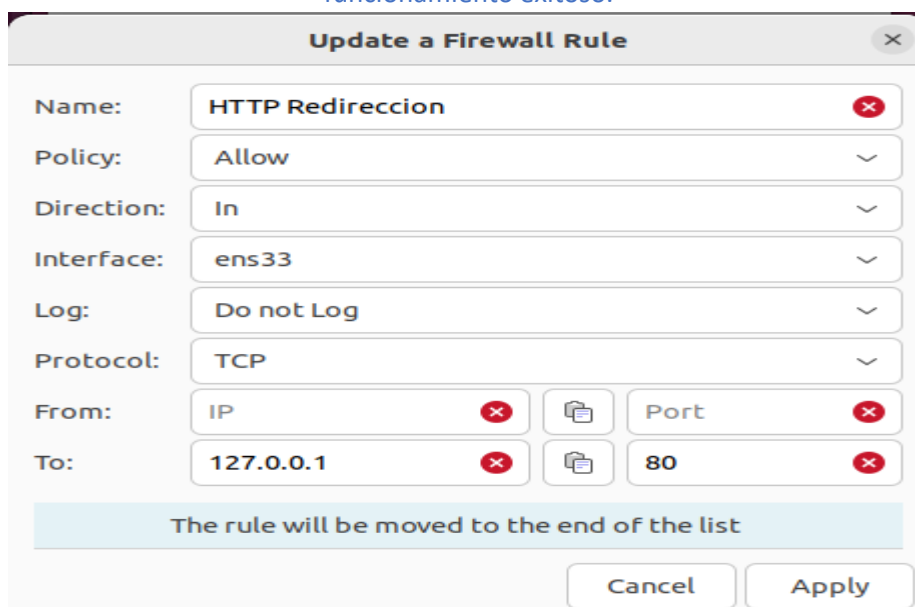


Ilustración 56 Regla necesaria por la interfaz gráfica GFW

En primer lugar, debemos agregar la regla necesaria para permitir conexiones desde internet que lleguen al servidor de la máquina virtual, mediante el uso del puerto 80 para HTTP. Vemos que con la regla no es suficiente y además de la regla se debe agregar un comando que es el que se muestra en la siguiente captura con el objetivo de conseguir redirigir todo el tráfico HTTP por la interfaz ens33 tal y como se muestra en la captura hacia la interfaz de loopback.

```
user@user-virtual-machine: $ sudo iptables -t nat -D POSTROUTING -o ens33 -p tcp --sport 80 -j SNAT --to-source 192.168.139.128
```

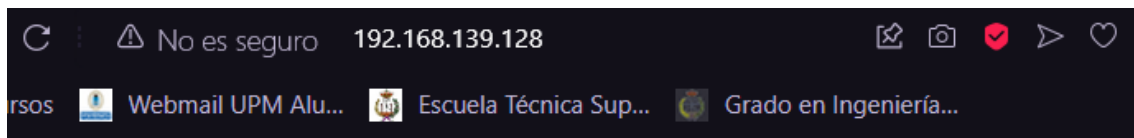
Ilustración 57 Comando necesario de introducir por comandos UFW

Como vemos este comando podría ser sustituido por la regla agregada de manera gráfica con GFW, de ambas formas se ha conseguido que funcione correctamente.

```
user@user-virtual-machine: $ sudo iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 80 -j DNAT --to-destination 127.0.0.1:80
```

Ilustración 58 Comando alternativo a interfaz gráfica GFW

Una vez introducido el comando ya nos permite el acceso a la interfaz del servidor.



# Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

*Ilustración 59 Captura Acceso desde internet al servidor*