Ejercicios Seminario 3

Por Arturo Cortés Sánchez

- Creo una solicitud de firma de certificado con

  ```
  openssl req -out certificado.csr -key ppkey -new
  ```

- Auto firmo el certificado con

  ```
  openssl x509 -out certificado2 -days 30 -signkey ppkey -req -in certificado.csr
  ```

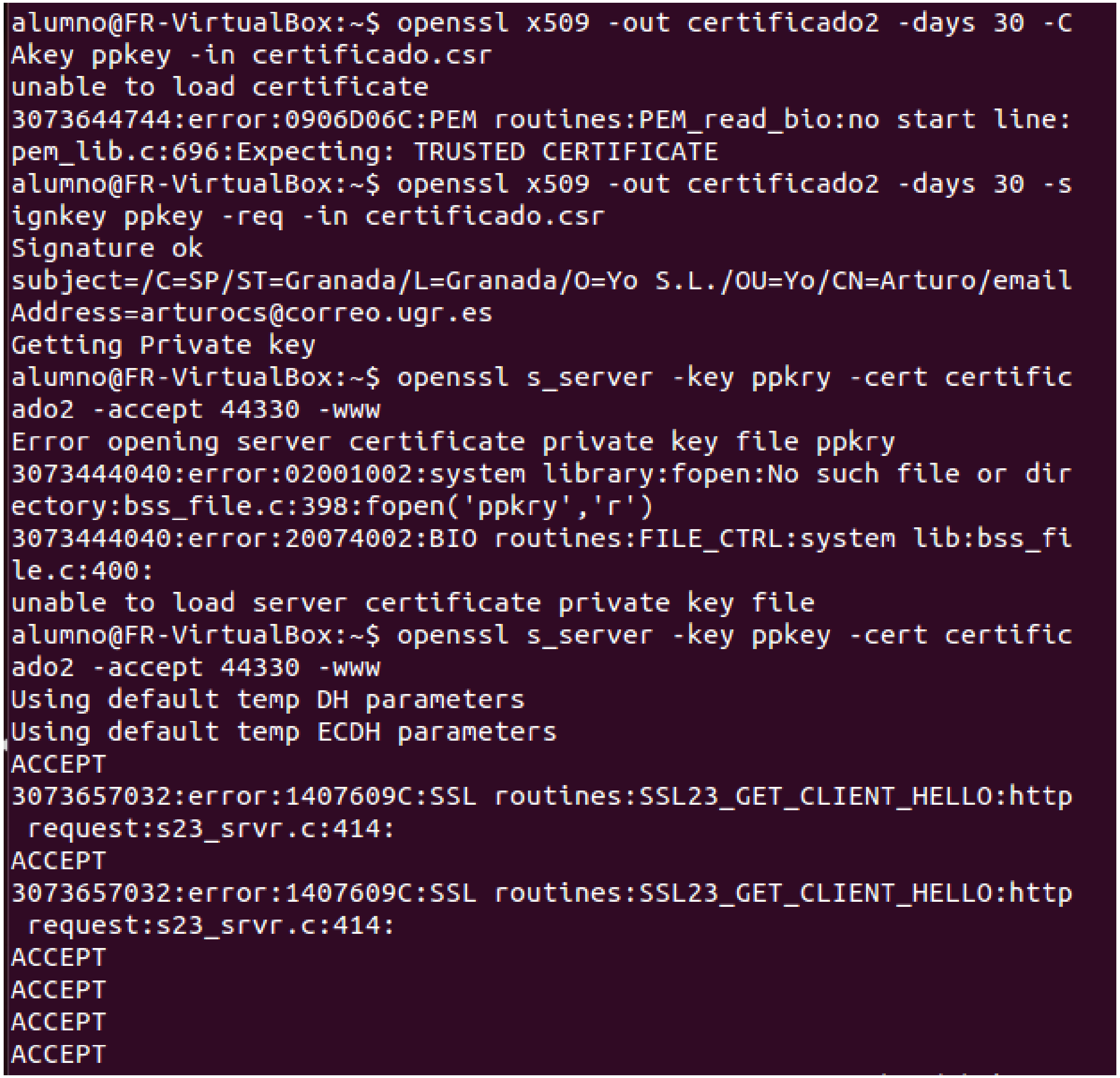
- Creo un servidor ssl con

  ```
  openssl s_server -key ppkey -cert certificado2 -accept 44330 -www
  ```

- Uso un cliente ssl para escuchar la conexión desde la otra maquina virtual

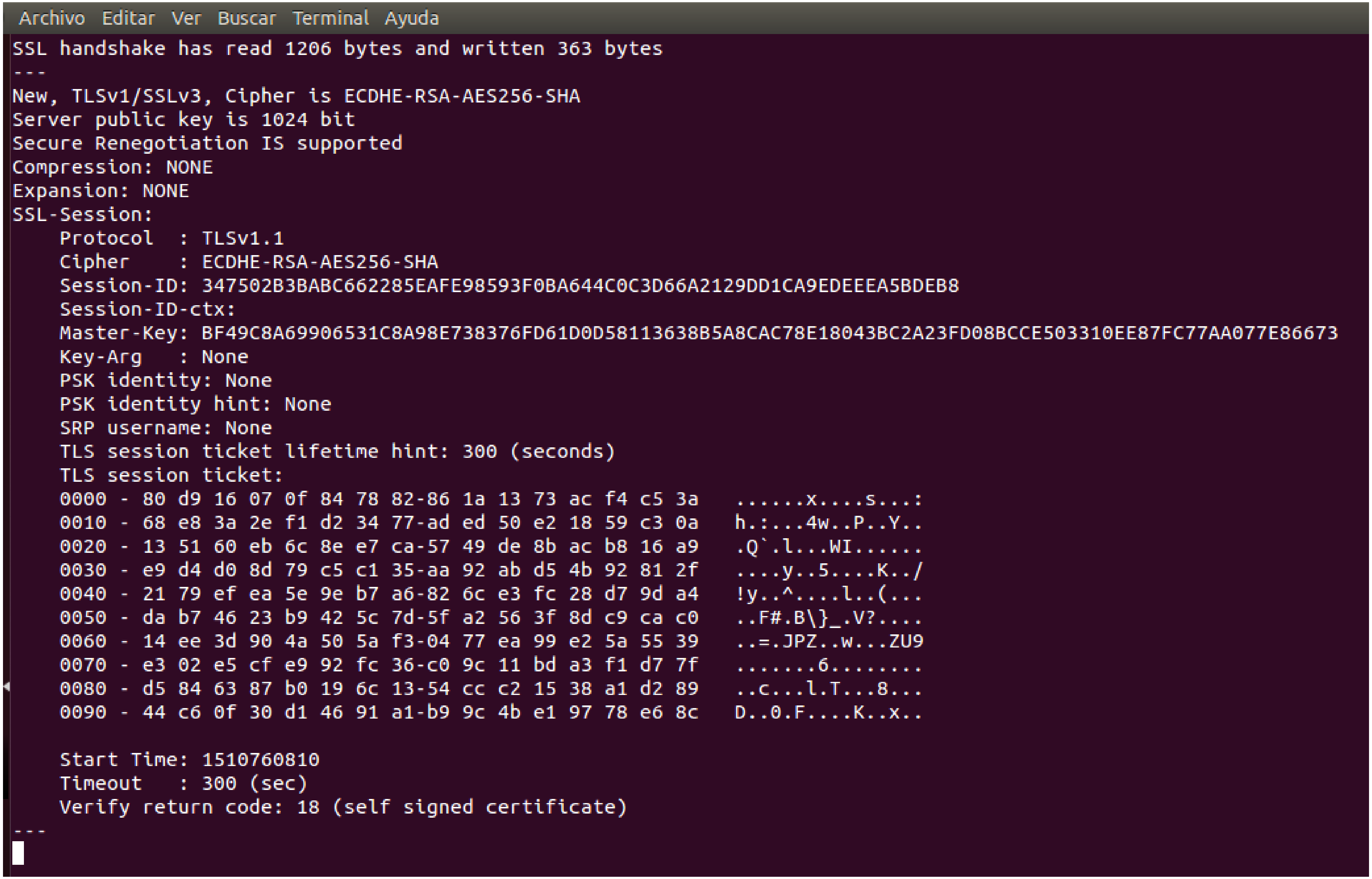
  ```
  openssl s_client -connect 10.0.2.5:44330
  ```

Máquina virtual servidor



```
alumno@FR-VirtualBox:~$ openssl x509 -out certificado2 -days 30 -C
Akey ppkey -in certificado.csr
unable to load certificate
3073644744:error:0906D06C:PEM routines:PEM_read_bio:no start line:
pem_lib.c:696:Expecting: TRUSTED CERTIFICATE
alumno@FR-VirtualBox:~$ openssl x509 -out certificado2 -days 30 -s
ignkey ppkey -req -in certificado.csr
Signature ok
subject=/C=SP/ST=Granada/L=Granada/O=Yo S.L./OU=Yo/CN=Arturo/email
Address=arturocs@correo.ugr.es
Getting Private key
alumno@FR-VirtualBox:~$ openssl s_server -key ppkry -cert certific
ado2 -accept 44330 -www
Error opening server certificate private key file ppkry
3073444040:error:02001002:system library:fopen:No such file or dir
ectory:bss_file.c:398:fopen('ppkry','r')
3073444040:error:20074002:BIO routines:FILE_CTRL:system lib:bss_fi
le.c:400:
unable to load server certificate private key file
alumno@FR-VirtualBox:~$ openssl s_server -key ppkey -cert certific
ado2 -accept 44330 -www
Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
3073657032:error:1407609C:SSL routines:SSL23_GET_CLIENT_HELLO:http
 request:s23_srvr.c:414:
ACCEPT
3073657032:error:1407609C:SSL routines:SSL23_GET_CLIENT_HELLO:http
 request:s23_srvr.c:414:
ACCEPT
ACCEPT
ACCEPT
ACCEPT
```

Máquina virtual cliente



```
SSL handshake has read 1206 bytes and written 363 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID: 347502B3BABC662285EAFE98593F0BA644C0C3D66A2129DD1CA9EDEEEA5BDEB8
    Session-ID-ctx:
    Master-Key: BF49C8A69906531C8A98E738376FD61D0D58113638B5A8CAC78E18043BC2A23FD08BCCE503310EE87FC77AA077E86673
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 80 d9 16 07 0f 84 78 82-86 1a 13 73 ac f4 c5 3a   ......x....s...:
    0010 - 68 e8 3a 2e f1 d2 34 77-ad ed 50 e2 18 59 c3 0a   h.:...4w..P..Y..
    0020 - 13 51 60 eb 6c 8e e7 ca-57 49 de 8b ac b8 16 a9   .Q`.l...WI......
    0030 - e9 d4 d0 8d 79 c5 c1 35-aa 92 ab d5 4b 92 81 2f   ....y..5....K../
    0040 - 21 79 ef ea 5e 9e b7 a6-82 6c e3 fc 28 d7 9d a4   !y..^....l..(...
    0050 - da b7 46 23 b9 42 5c 7d-5f a2 56 3f 8d c9 ca c0   ..F#.B\}_.V?....
    0060 - 14 ee 3d 90 4a 50 5a f3-04 77 ea 99 e2 5a 55 39   ..=.JPZ..w...ZU9
    0070 - e3 02 e5 cf e9 92 fc 36-c0 9c 11 bd a3 f1 d7 7f   .......6........
    0080 - d5 84 63 87 b0 19 6c 13-54 cc c2 15 38 a1 d2 89   ..c...l.T...8...
    0090 - 44 c6 0f 30 d1 46 91 a1-b9 9c 4b e1 97 78 e6 8c   D..0.F....K..x..

    Start Time: 1510760810
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
```