

A1 – Telnet SMTP

Amb telnet ja no es pot fer servir gmail ja que Google va implementar la obligació d'establir la connexió encriptada per TLS, llavors no es pot fer a no ser que tinguem el telnet actualitzat amb capacilitat de ssl.

Per tant la forma actual de poder fer-ho és amb open ssl:

**Es poden fer servir dos ports per establir la connexió, amb el port 587 (fa servir el protocol TLS) o amb el port 456 (fa servir el protocol SSL).*

En el meu cas he fet servir el port 587, és a dir faré servir el protocol TLS:

1) Realitzar la connexió al servidor de, en el meu cas, gmail

```
--id=ddlelocalhost --js openssl s_client -starttls smtp -connect smtp.gmail.com:587 ---crlf
CONNECTED(00000000)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 101
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = smtp.gmail.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = smtp.gmail.com
   i:C = US, O = Google Trust Services, CN = GTS CA 101
 1 s:C = US, O = Google Trust Services, CN = GTS CA 101
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----
Server certificate
-----BEGIN CERTIFICATE-----
MIIEFzCCA6I+gAwIBAgIRAO3YlIpK/5SIAwAAEQLQH8WdQVJKoZitHvcNAQELBQAww
OjLMakGA1UEBHMCVVhhAcBgNVBAU0TUDubm9udGtzc2RScnNvdCZvZDkxM2JXZWlnZET
MBEGA1UEAxMKMRIRTENIDFPMTAEFwMyTAHMjbWYoOTA1MThtaFAwOTAMGMjAwOTA1
MTdaMGCGZAzBgNVBAYTA1VTMRMcWqdVQQIEwdYXpxZm9ybmlHRMYWVyAFVDQHQw
bxWNrLmdtYWJsLnMbTBMRBMGByqGSMA49EGGCgsM49EAWEAHiABBBMZczFTFH/
dUsLVzhvbFYewux/O2WGtb48AGMLM3euzvt+rDtqZIMVN48THOEJ3FcKycriy3FPpc
+O+Wcx9ihIKgjkgzwbiICVCzAoBGUNHQBHA8FEABMACB4AwEWdvRoLBAmwCcPIkwBV
BOUHAWEdAyDVROGTaqBI/AiwAdABgnvNHQ4EFgQU8TRDAUFILCD+iMiqlTLuirRCoe
rbAHwhYDVRObjBBgwFoAUmh4bhDrZvsy3JVkyVG630j/SswAiKWbyBBQUHAREEE
XDCAmcGCCscGAQuFBzAbhh9ndRhWo18bv2NZcc5wa2kuZZyn9dhMDhmxbzfj33l
CCSCGCCsgACGaUBFzbAch9ndRhwo18vgctPmbld2cvZ3NyMH9VFHXMTzeUy3JMBlKG
AIjdEQSQSBMcCDDntdHAUzz1tlawHuWTy9tFCGALIdUAQMbgCyAGYZ4EMAQTCAWAwg
CIAAQOBInkbCBQMWydVRORbfBCwkvjAocCaGIJIYAHHRpDovLY2NbYCsbKuZ29vv
zyHVFMFXtzFzj33lLMneylBDCCAQMGCISgaQOLknICAIEFGFeafTWB2AHO+-8viPl
yhVaCTcmqeUoiLSKU8eoAl/LmqKaJl+vTXOAABBdz4nm18AAAQDAQCEARQITgpjNg
tzs/EDOpEPThJwier1/kAhSiH4xzMS3Lv+F2glQC1CQTLIXSEGVJMVMv4dc+zciXIqx
zgQEIVFLPONiyGFSP2pkUmB1Afzc05+5qtFRLLCFMQenRWSh5A+x9GR9yhc5SYklbz
7CKAACsd4zmmyAAAAQDEayNRaiQiGLIFt9QM9grtm2xp9+ySwfsLDlvbtZEszPD
7ckVmmsCIFfy8htlwAKAPoxCiGoivEU90uyaaobVBzt416jfwMAOGCSogSI03
DHXCeqCUAA4IBAQDEh3xrtpjSmjlbhwERTGTvmnzZgvSehzcsyk4_0AhdHYdygmxi
KH4x63JaTrYEychor1vxg4Ba1/KiemPd3cgdpbehezkPC/Bqadsl5VoNDGDZ
pSaumy2hpToDFLIimLOmgPGHio1vlLucdqBLkvf6psksktOKTGZZzdofdnJhi
Zon8f9SMXLQxywnYnhilUhkyHo9f6s0cmcTv+hMFxfxCwi1DETIN6fgNcvLCQRkq3
RHGfotWh+m-netdezqViwl/TJPz3smgtRGPR-hpa3fJanANMUQCeVNaooznCrfrpgEtE4k
NDWydwObErj89XLpc6kj/EJPOPAwpirEOD01968
-----END CERTIFICATE-----
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = smtp.gmail.com
-----
issuer=C = US, O = Google Trust Services, CN = GTS CA 101
-----
No client certificate has names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
-----
SSL handshake has read 2890 bytes and written 421 bytes
Verification: OK
```

```

---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
250 SMTPUTF8

```

Com podem veure faig servir l'ordre:

```
openssl s_client -starttls smtp -connect smtp.gmail.com:587 -crlf
```

- starttls → Farem servir el protocol de seguretat incorporat per google
- crlf → Ens permetrà després poder acabar el missatge amb un “.”

2) Ara hem dir «hola», ho podem fer amb helo o ehlo (aquesta dona més info), en el meu cas l'he fet amb ehlo

```
ehlo gmail.com
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol    : TLSv1.3
  Cipher      : TLS_AES_256_GCM_SHA384
  Session-ID: D3DD21B888A553986C166B721E16857AF97A764A243FD840FB466DD92E05A9F1
  Session-ID-ctx:
  Resumption PSK: AF07BB0BD1AFE48F80A6040222FA47665282F274EAD4AF716A843350EBF4178D45547BE18C296829AB8EF02DC4D46AFE
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 172800 (seconds)
  TLS session ticket:
0000 - 01 94 68 e7 45 a1 a3 3d-65 9b ac 25 cf cb fe 33    ..h.E..=e..%...3
0010 - 50 b6 1b 1d 18 a4 18 37-4c df 70 8b f4 9a f3 1a    P.....7L.p....
0020 - 09 d3 d0 3f a0 49 a5 61-39 d0 73 9f b4 ec 52 5b    ...?.I.a9.s...R[
0030 - d4 bf 18 cb 67 35 c2 6a-b8 35 db 40 20 52 c2 07    ....g5.j.5.@ R..
0040 - fe 8a 3f 95 d2 d8 a6 7a-eb cd 0b aa e6 79 cc 9c    ..?...Z....y..
0050 - 9d 19 21 51 da 37 eb e6-9b ad 71 c1 0e 58 f3 ed    ..!Q.7....q..X..
0060 - 53 77 c6 e3 dd c8 4f fe-d2 e2 08 51 62 12 c6 47    Sw....0....Qb..G
0070 - 22 5a 9e 0a 1c 22 1f e2-60 d7 71 67 a3 8b 69 19    "Z..."`..qg..i.
0080 - 35 75 78 8a fb c1 ec 29-1b 25 7e dd d6 21 c3 07    5ux....).%~!...
0090 - 60 49 a8 48 a6 43 46 70-d0 23 ea 2c 72 2a 04 b7    `I.H.CFp.#.,r*..
00a0 - bf 33 46 f0 c2 50 ad 42-5c 38 46 1e b6 5f b8 d5    .3F..P.B\8F...
00b0 - b7 a9 39 c4 3a d3 f4 cc-f4 1b 8c dc 65 c8 2e 8a    .9:.....e...
00c0 - bd 1f b1 82 6f 69 0e df-55 60 5e 81 48 8e 51 21    ....oi...U'^.H.Q!
00d0 - 11 00 42 42 d9 dc 46 92-39 ad 4c 33 6e f4 4f 78    ..BB..F.9.L3n.Ox
00e0 - c7 c1 b0 b5 d8 3e ab 89-dd 34 63 d3            ....>...4c.

  Start Time: 1614190026
  Timeout    : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: no
  Max Early Data: 0
---
```

```
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol    : TLSv1.3
  Cipher      : TLS_AES_256_GCM_SHA384
  Session-ID: 239AF5727050D85B6EEA45FC3CC5EC89E903BEEC1A90C86E7D9DFF6815C22E83
  Session-ID-ctx:
  Resumption PSK: 43BF0464EDB3D376918C7AB098DD5EEDE1820925CE55BCA152DBB3E414CDA0852A072402A38D7063EA6379B44FA8DDF
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 172800 (seconds)
  TLS session ticket:
0000 - 01 94 68 e7 45 a1 a3 3d-65 9b ac 25 cf cb fe 33    ..h.E..=e..%...3
0010 - 6b ab 44 96 2a 98 73 47-ac 62 2c c4 fc 3a 5f 0e    k.D.*.sG.b,..._.
0020 - ac 2e 24 e5 32 23 f5 ec-e1 ef 52 46 5d 7b 42 58    ..$.2#....RF){BX
0030 - d3 1a 2b f0 4d 1d 29 10-f8 63 90 94 67 3b 80 18    ..+.M.)...c..g;..
0040 - 77 cf 6e 3d df 92 2d 9e-bd 4a 90 51 bf a3 66 b3    w.n=...-.J.Q..f.
0050 - fc 2b c4 0f da a5 59 17-f7 3c ba 76 d9 b5 ab 9b    .+....V...<.v....
0060 - 2f 84 44 f1 b7 1c 86 a0-3b 9f 5b f1 65 96 1b 86    /.D.....;.[.e...
0070 - 33 73 f7 48 bf 0e d7 ce-59 50 c2 85 62 1d 7d 43    3s.H....YP..b.)C
0080 - 2f 5d 1e 5e 0b db eb 33-09 f7 ff b3 5c 85 d6 e8    /].^...3....\...
0090 - 6f f0 2b 88 8c be ed 0d-8a a5 ec f1 9b b4 c6 d9    o.+.....
00a0 - 65 c8 a8 08 bf 23 65 24-ac a0 bf b3 db c0 4a da    e.....#e$.....J.
00b0 - 58 b5 b8 11 b4 a9 f2 ad-76 17 50 0d 2d b5 0e ec    X.....v.P.-...
00c0 - ed d2 50 c0 fd 91 32 12-a2 09 3a b3 71 bb f4 10    ..P...2....q...
00d0 - c4 00 95 88 36 1d fb 89-f6 8d da e1 b2 41 90 97    ....6.....A...
00e0 - b2 0d c7 48 2f 92 cf 58-ff cb 8a 4a            ...H/..X...J

  Start Time: 1614190026
  Timeout    : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: no
  Max Early Data: 0
---
```

```
read R BLOCK
250-smtp.gmail.com at your service, [37.223.121.230]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
```

3) Ara hem de fer el login, com veiem hi ha bastants formes de fer login, jo faré servir el **auth login**:

***Per poder l'usuari i contrasenya haurem de generar aquests en un encriptació a base 64:**

```
[didi@localhost ~]$ echo -ne "sanchezpiedradiego" | base64
c2FuY2hlenBpZWRYYWRpZWdv
```

7G11ZCENSOREDMDA=

```
auth login
334 VXNlcm5hbWU6
c2FuY2hlenBpZWRYYWRpZWdv
334 UGFzc3dvcmQ6
CENSORED
535-5.7.8 Username and Password not accepted. Learn more at
535 5.7.8 https://support.google.com/mail/?p=BadCredentials t7sm3733875wmq.44 - gsmt
```

Com podem veure ens dona un error, això es degut a que la majoria de la gent té una opció al seu compte de google que no permet la connexió des de dispositius que google pren per insegurs, llavors hem d'activar l'opció que permet la connexió:

← Acceso de aplicaciones poco seguras

Algunos dispositivos y aplicaciones utilizan una tecnología de inicio de sesión poco segura, lo que aumenta la vulnerabilidad de tu cuenta. Te recomendamos que desactives el acceso de estas aplicaciones, aunque también puedes activarlo si quieres usarlas a pesar de los riesgos que conllevan. Desactivaremos este ajuste de forma automática si no lo utilizas. [Más información](#)

Permitir el acceso de aplicaciones poco seguras: Sí



Ara tornem a provar:

```
auth login
334 VXNlcm5hbWU6
c2FuY2hlenBpZWRYYWRpZWdv
334 UGFzc3dvcmQ6
ZGllZ3VpbjE3MzIwMDA=
235 2.7.0 Accepted
```

Ara si!

4) Ara només queda enviar el missatge:

```
mail from: <sanchezpiedradiago@gmail.com>
250 2.1.0 OK t7sm3733875wmq.44 - gsmt
rcpt to: <sanchezpiedradiago@gmail.com>
250 2.1.5 OK t7sm3733875wmq.44 - gsmt
data
354 Go ahead t7sm3733875wmq.44 - gsmt
hola
esto es una prueba de mensaje!
.
250 2.0.0 OK 1614190824 t7sm3733875wmq.44 - gsmt
```

5) Per últim comprovem que ens ha arribat el missatge:

