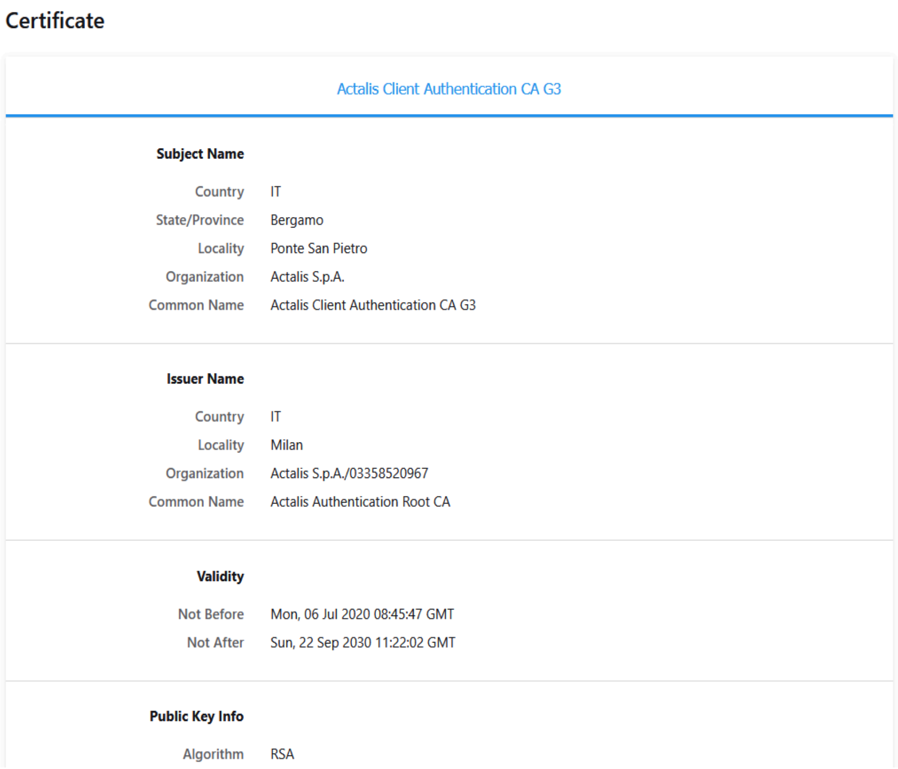
496 Homework - 2
Özlem Kılıçkıran
Emircan Kılıçaslan

Q1-

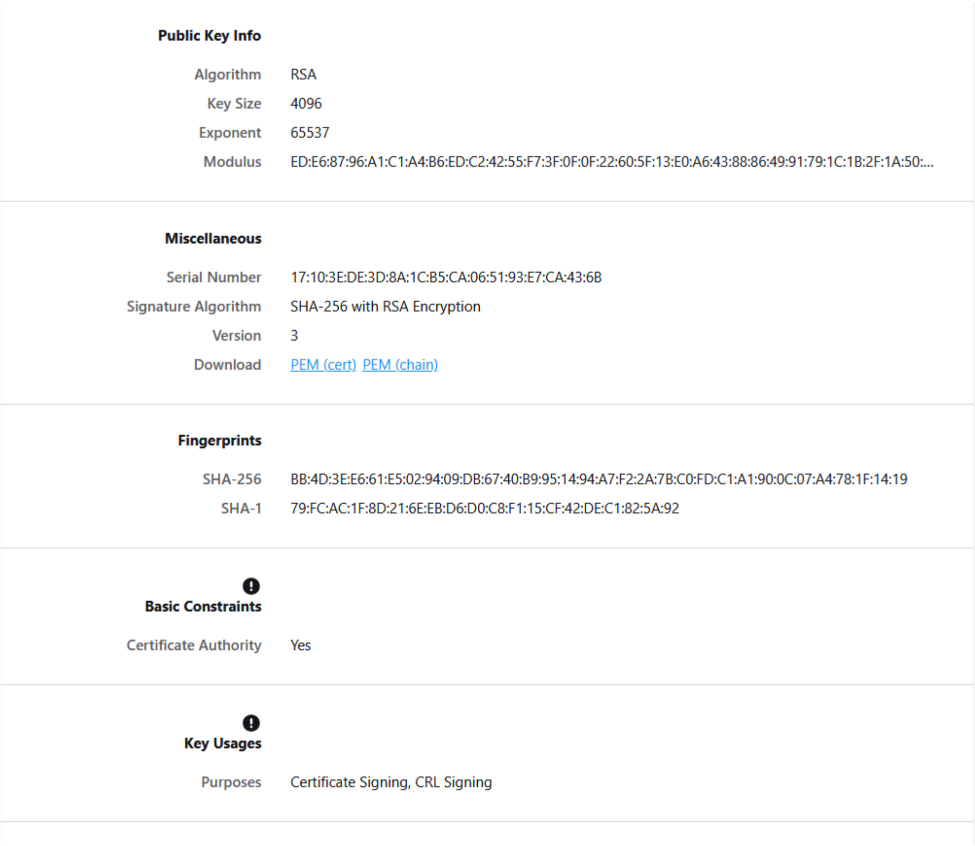
Emircan’s certificate:



Certificate

Actalis Client Authentication CA G3

Subject Name	
Country	IT
State/Province	Bergamo
Locality	Ponte San Pietro
Organization	Actalis S.p.A.
Common Name	Actalis Client Authentication CA G3
Issuer Name	
Country	IT
Locality	Milan
Organization	Actalis S.p.A./03358520967
Common Name	Actalis Authentication Root CA
Validity	
Not Before	Mon, 06 Jul 2020 08:45:47 GMT
Not After	Sun, 22 Sep 2030 11:22:02 GMT
Public Key Info	
Algorithm	RSA



Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	ED:E6:87:96:A1:C1:A4:B6:ED:C2:42:55:F7:3F:0F:0F:22:60:5F:13:E0:A6:43:88:86:49:91:79:1C:1B:2F:1A:50:...

Miscellaneous

Serial Number	17:10:3E:DE:3D:8A:1C:B5:CA:06:51:93:E7:CA:43:6B
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

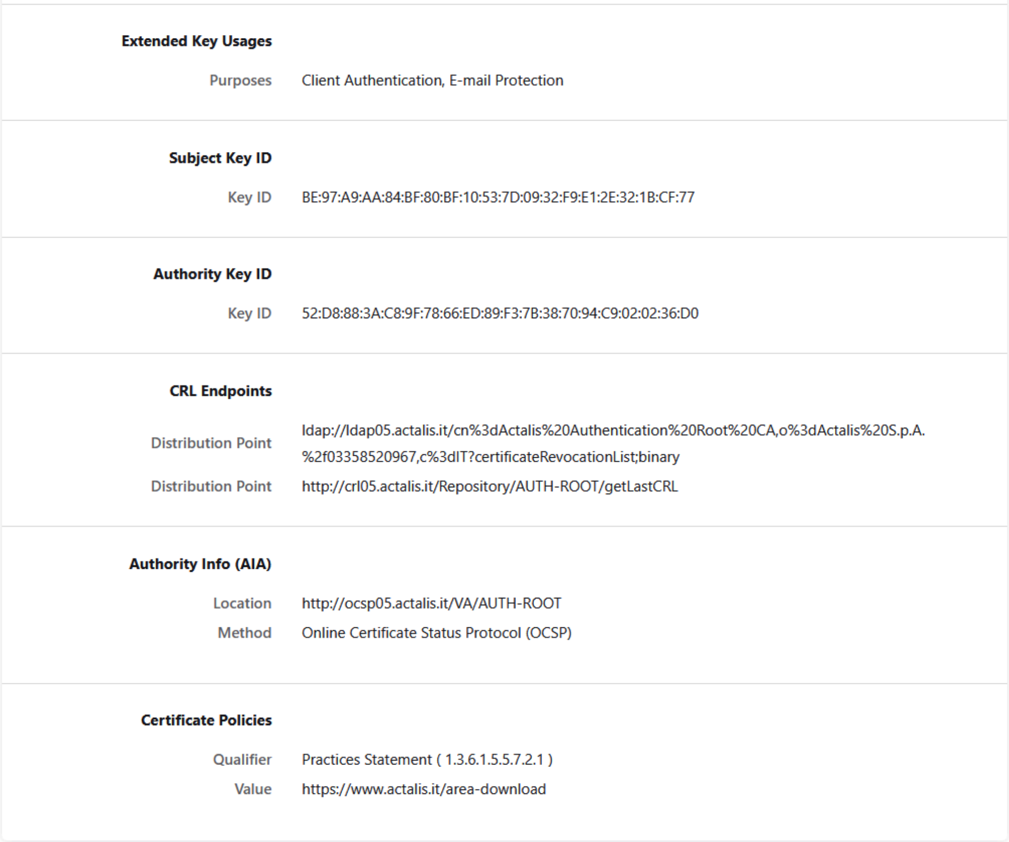
SHA-256	BB:4D:3E:E6:61:E5:02:94:09:DB:67:40:B9:95:14:94:A7:F2:2A:7B:C0:FD:C1:A1:90:0C:07:A4:78:1F:14:19
SHA-1	79:FC:AC:1F:8D:21:6E:EB:D6:D0:C8:F1:15:CF:42:DE:C1:82:5A:92

❗
Basic Constraints

Certificate Authority	Yes

❗
Key Usages

Purposes	Certificate Signing, CRL Signing



Extended Key Usages

Purposes	Client Authentication, E-mail Protection

Subject Key ID

Key ID	BE:97:A9:AA:84:BF:80:BF:10:53:7D:09:32:F9:E1:2E:32:1B:CF:77

Authority Key ID

Key ID	52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0

CRL Endpoints

Distribution Point	ldap://ldap05.actalis.it/cn%3dActalis%20Authentication%20Root%20CA,o%3dActalis%20S.p.A.%2f03358520967,c%3dIT?certificateRevocationList;binary
Distribution Point	http://crl05.actalis.it/Repository/AUTH-ROOT/getLastCRL

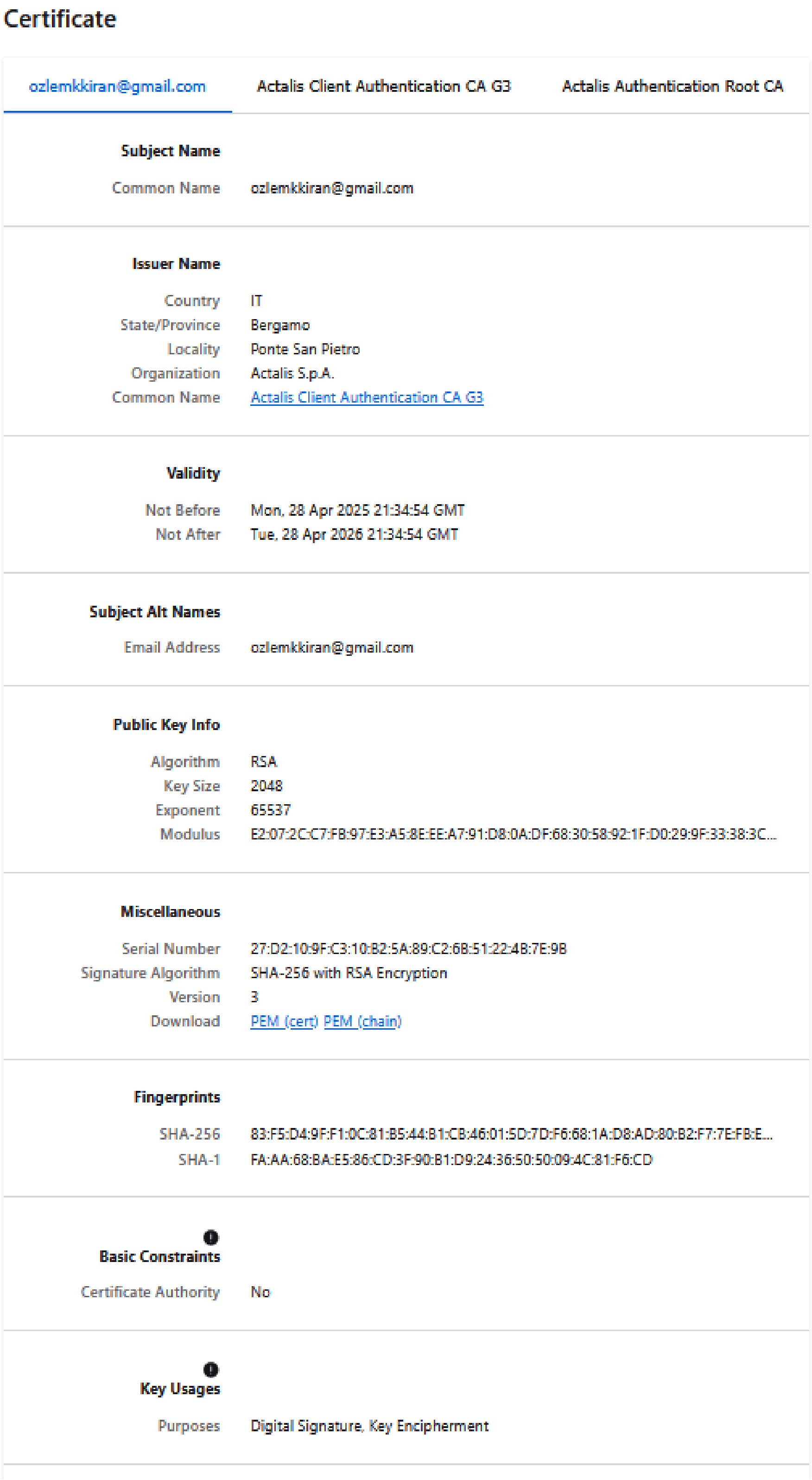
Authority Info (AIA)

Location	http://ocsp05.actalis.it/VA/AUTH-ROOT
Method	Online Certificate Status Protocol (OCSP)

Certificate Policies

Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	https://www.actalis.it/area-download

Özlem's Certificate:



Certificate

ozlemkkiran@gmail.com
Actalis Client Authentication CA G3
Actalis Authentication Root CA

Subject Name

Common Name	ozlemkkiran@gmail.com

Issuer Name

Country	IT
State/Province	Bergamo
Locality	Ponte San Pietro
Organization	Actalis S.p.A.
Common Name	Actalis Client Authentication CA G3

Validity

Not Before	Mon, 28 Apr 2025 21:34:54 GMT
Not After	Tue, 28 Apr 2026 21:34:54 GMT

Subject Alt Names

Email Address	ozlemkkiran@gmail.com

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	E2:07:2C:C7:FB:97:E3:A5:8E:EE:A7:91:D8:0A:DF:68:30:58:92:1F:D0:29:9F:33:38:3C...

Miscellaneous

Serial Number	27:D2:10:9F:C3:10:B2:5A:89:C2:6B:51:22:4B:7E:9B
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

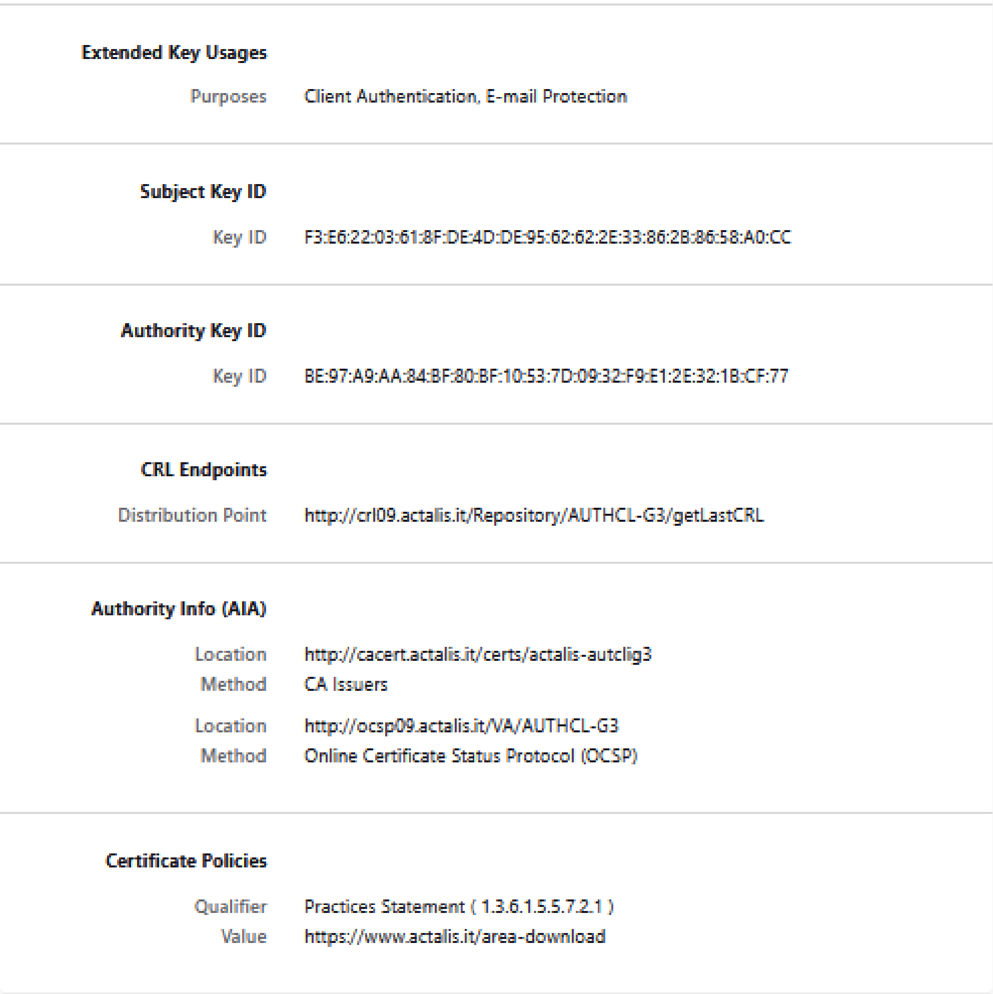
SHA-256	83:F5:D4:9F:F1:0C:81:B5:44:B1:CB:46:01:5D:7D:F6:68:1A:D8:AD:80:B2:F7:7E:FB:E...
SHA-1	FA:AA:68:BA:E5:86:CD:3F:90:B1:D9:24:36:50:50:09:4C:81:F6:CD

Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Key Encipherment



Extended Key Usages

Purposes	Client Authentication, E-mail Protection

Subject Key ID

Key ID	F3:E6:22:03:61:8F:DE:4D:DE:95:62:62:2E:33:86:2B:86:58:A0:CC

Authority Key ID

Key ID	BE:97:A9:AA:84:BF:80:BF:10:53:7D:09:32:F9:E1:2E:32:1B:CF:77

CRL Endpoints

Distribution Point	http://crl09.actalis.it/Repository/AUTHCL-G3/getLastCRL

Authority Info (AIA)

Location	http://cacert.actalis.it/certs/actalis-autclig3
Method	CA Issuers
Location	http://ocsp09.actalis.it/VA/AUTHCL-G3
Method	Online Certificate Status Protocol (OCSP)

Certificate Policies

Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	https://www.actalis.it/area-download

Emircan's Certificate Details:

- **Issued by:** Actalis S.p.A.
- **Certificate Algorithm:** RSA
- **Key Length:** 4096 bits
- **Validity Period:** The certificate is valid from 2020 to 2030.

Özlem's Certificate Details:

- **Issued by:** Actalis S.p.A.
- **Certificate Algorithm:** RSA (with SHA-256 for signing: SHA-256 with RSA Encryption
- **Key Length:** 2048 bits
- **Validity Period:** From Mon, 28 Apr 2025 21:34:54 GMT to Tue, 28 Apr 2026 21:34:54 GMT

Question- "How can one view the details of issuer's (Certificate Authority of your certificate) certificate on Thunderbird?"

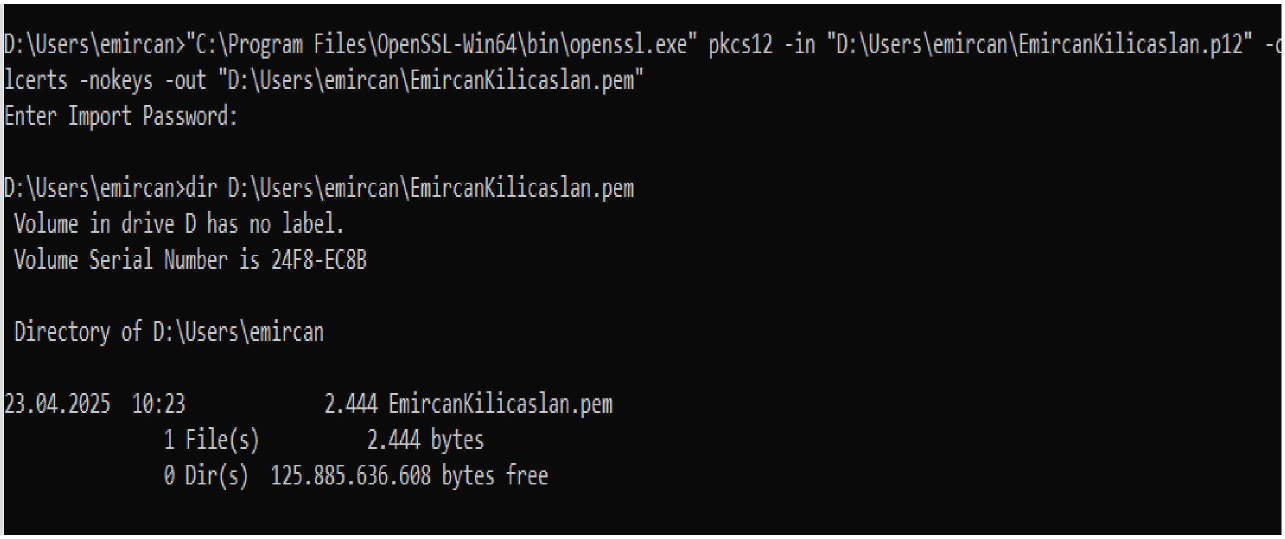
To view the details of the issuer's certificate (Certificate Authority), go to:

- **Thunderbird > Settings > Privacy & Security > Certificates > Manage Certificates**
- Switch to the **"Authorities"** tab
- Search for **"Actalis Authentication Root CA"** or similar
- Click on it and choose **"View"** to see details like:
    - Issuer name
    - Validity period
    - Fingerprints
    - Signature algorithm
    - Key usage and policies

Q2-

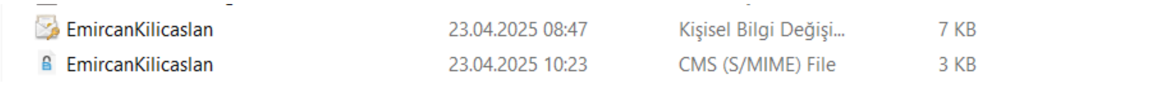
Emircan’s Screens:

Emircan’s terminal:

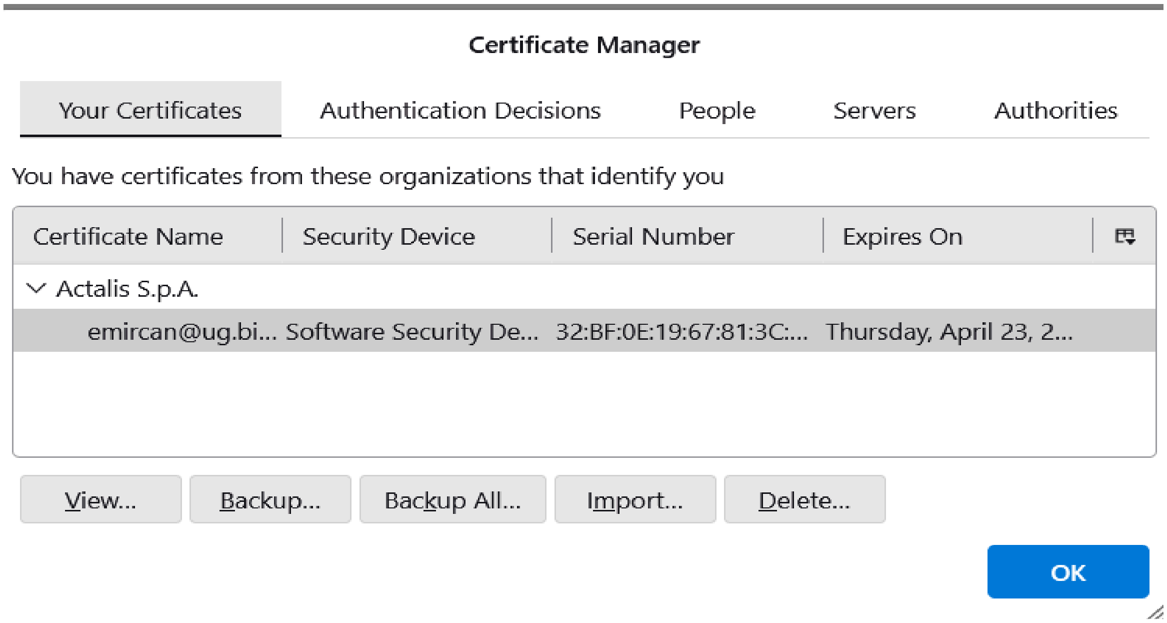


```
D:\Users\emircan>"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -in "D:\Users\emircan\EmircanKilicaslan.p12" -c
lcerts -nokeys -out "D:\Users\emircan\EmircanKilicaslan.pem"
Enter Import Password:

D:\Users\emircan>dir D:\Users\emircan\EmircanKilicaslan.pem
 Volume in drive D has no label.
 Volume Serial Number is 24F8-EC8B

 Directory of D:\Users\emircan

23.04.2025  10:23             2.444 EmircanKilicaslan.pem
               1 File(s)          2.444 bytes
               0 Dir(s)  125.885.636.608 bytes free
```

Emircan’s Certificate on Thunderbird:



EmircanKilicaslan	23.04.2025 08:47	Kişisel Bilgi Değişi...	7 KB
EmircanKilicaslan	23.04.2025 10:23	CMS (S/MIME) File	3 KB

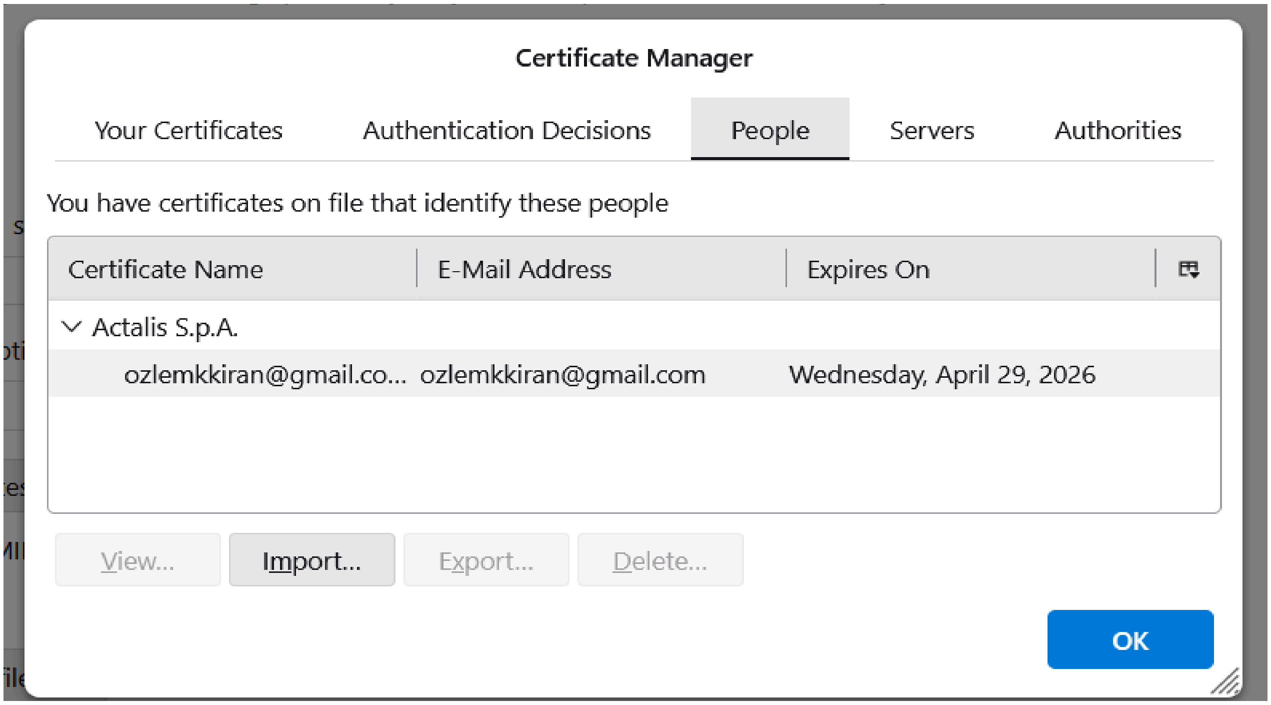


Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
Actalis S.p.A.			
emircan@ug.bi...	Software Security De...	32:BF:0E:19:67:81:3C:...	Thursday, April 23, 2...

Emircan’s Imported Certificate on Özlem’s Thunderbird:

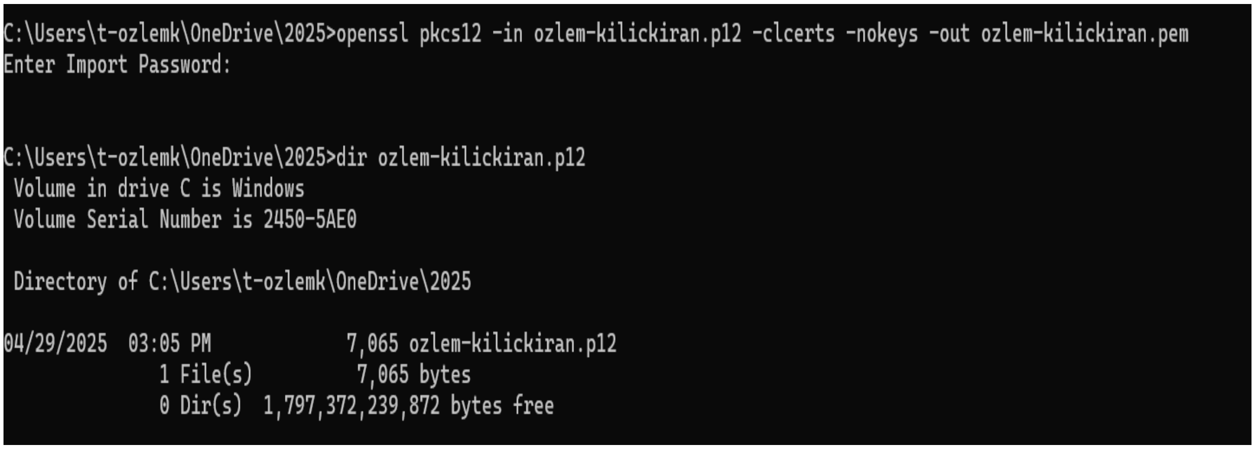


You have certificates on file that identify these people

Certificate Name	E-Mail Address	Expires On
Actalis S.p.A.		
ozlemkkiran@gmail.co...	ozlemkkiran@gmail.com	Wednesday, April 29, 2026

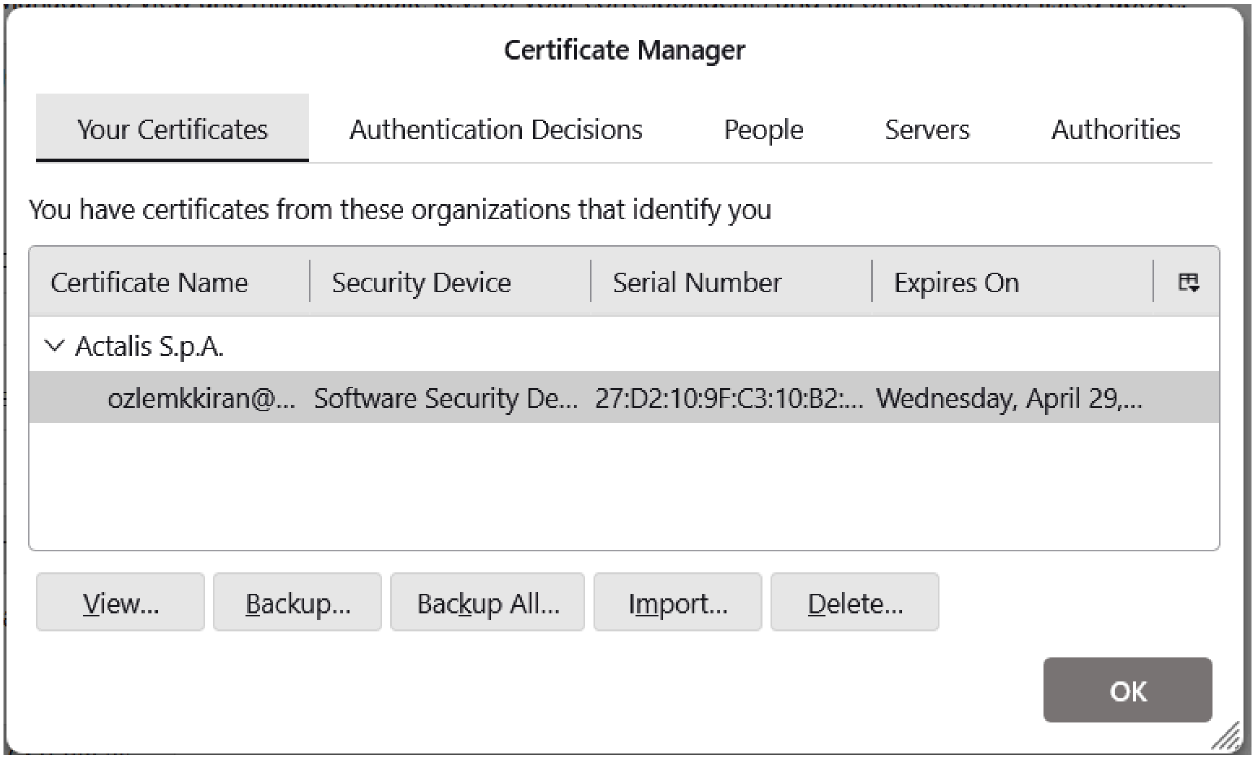
Özlem’s Screens:

Özlem’s terminal:



```
C:\Users\t-ozlemk\OneDrive\2025>openssl pkcs12 -in ozlem-kilickiran.p12 -clcerts -nokeys -out ozlem-kilickiran.pem
Enter Import Password:


C:\Users\t-ozlemk\OneDrive\2025>dir ozlem-kilickiran.p12
 Volume in drive C is Windows
 Volume Serial Number is 2450-5AE0

 Directory of C:\Users\t-ozlemk\OneDrive\2025

04/29/2025  03:05 PM             7,065 ozlem-kilickiran.p12
               1 File(s)          7,065 bytes
               0 Dir(s)  1,797,372,239,872 bytes free
```

Özlem’s Certificate on Thunderbird:

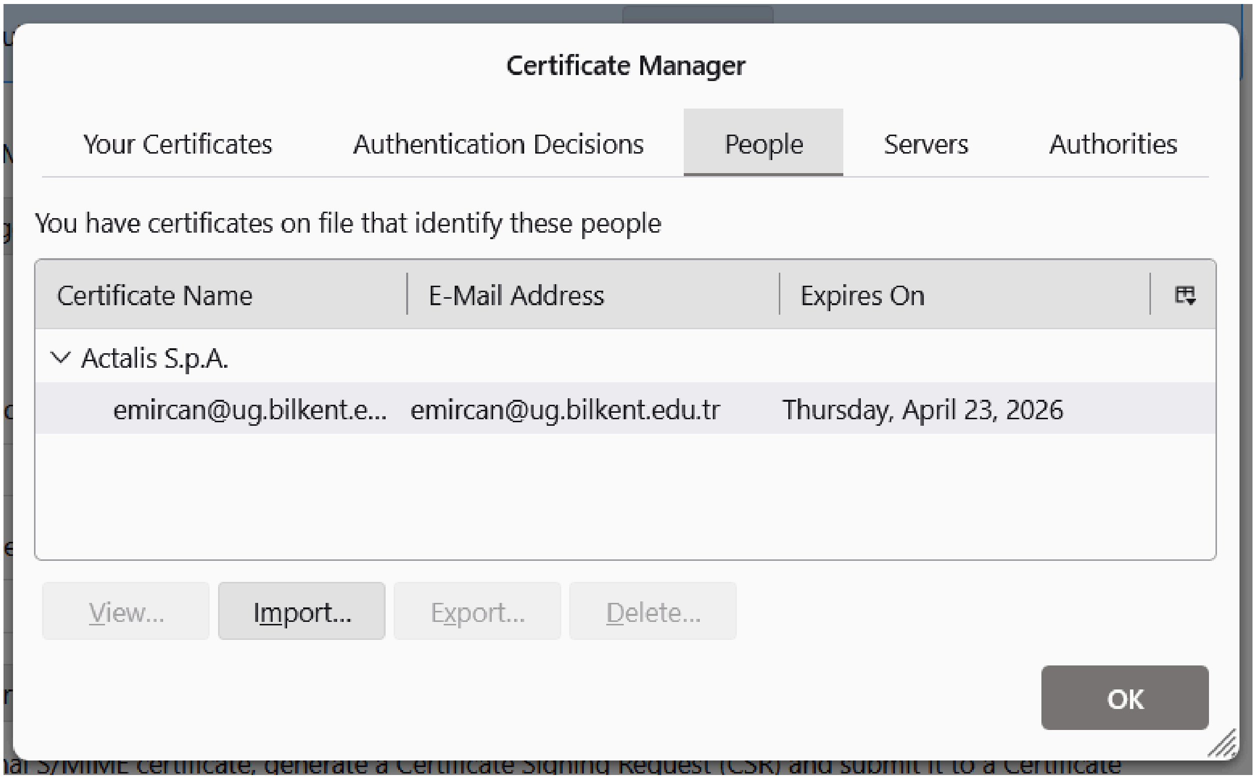


Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
Actalis S.p.A.			
ozlemkkiran@...	Software Security De...	27:D2:10:9F:C3:10:B2:...	Wednesday, April 29,...

Özlem’s Imported Certificate on Emircan’s Thunderbird:



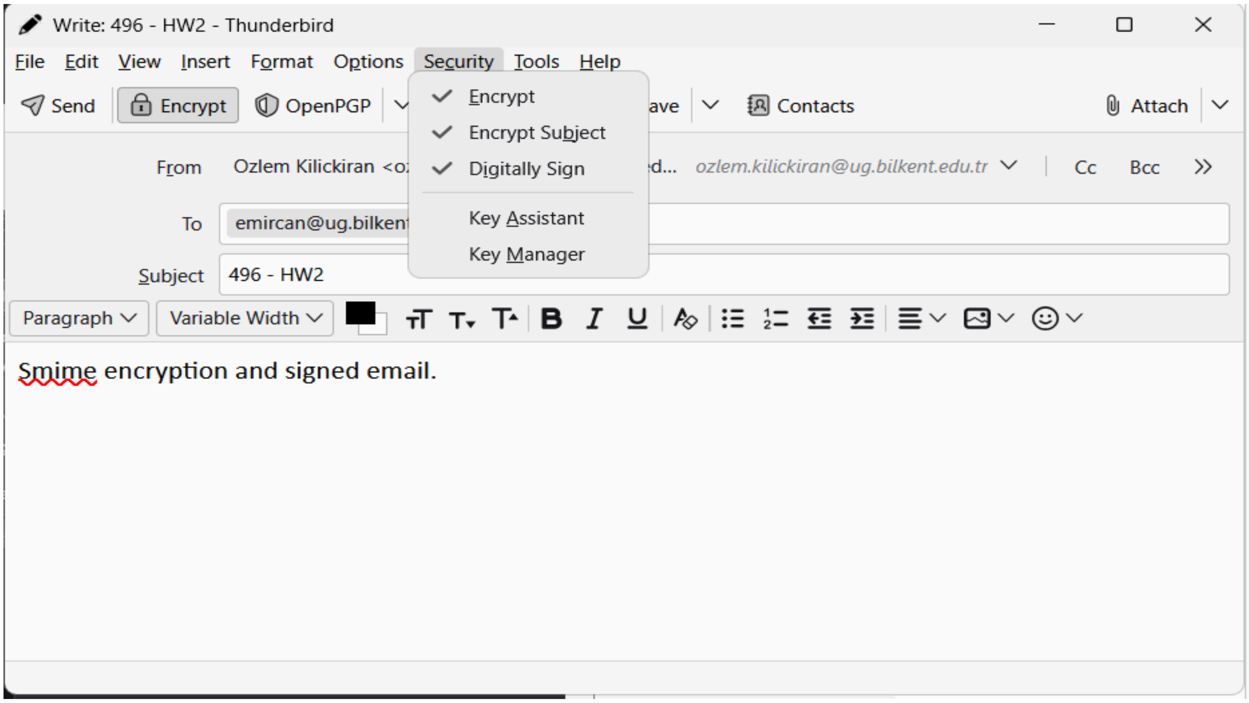
Certificate Manager

You have certificates on file that identify these people

Certificate Name	E-Mail Address	Expires On
Actalis S.p.A.		
emircan@ug.bilkent.e...	emircan@ug.bilkent.edu.tr	Thursday, April 23, 2026

EMAIL PART:

Özlem’s email sending screen on Thunderbird:



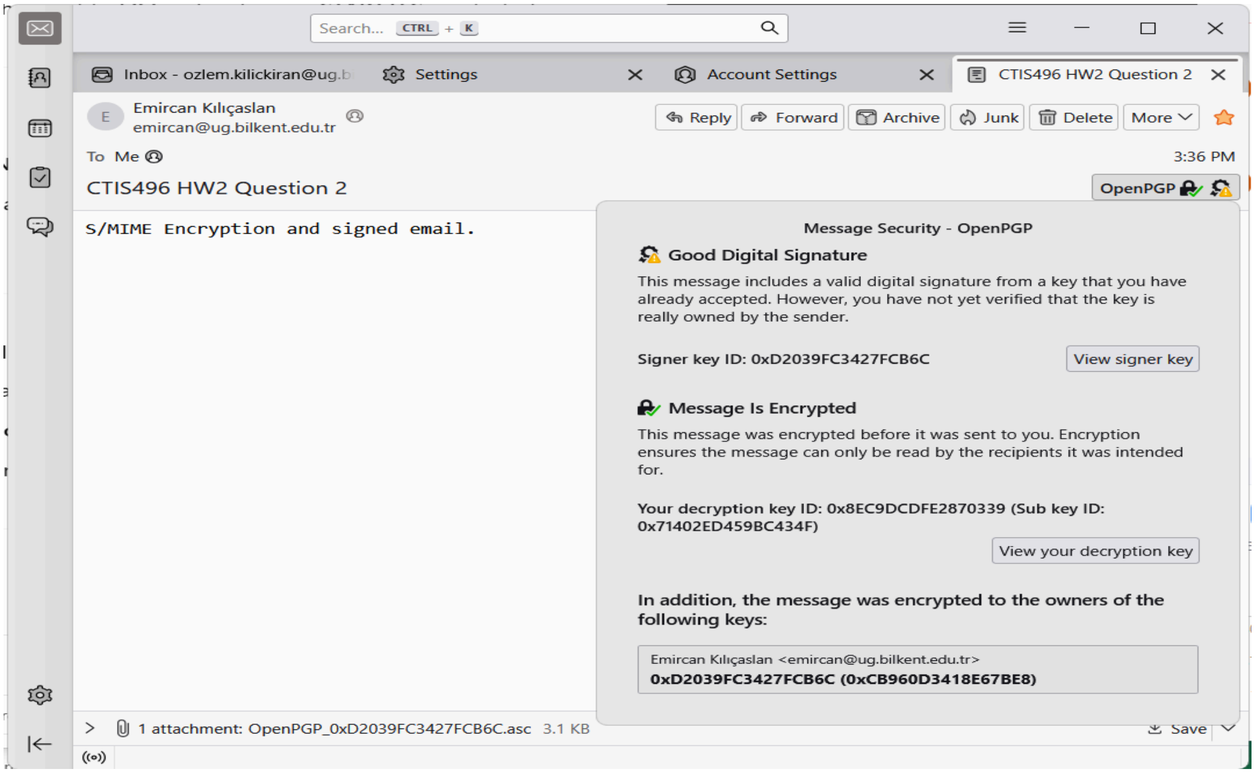
From Ozlem Kilickiran <o: ...d... ozlem.kilickiran@ug.bilkent.edu.tr

To emircan@ug.bilkent

Subject 496 - HW2

Smime encryption and signed email.

Özlem’s screen showing Emircan’s email on Thunderbird:



Emircan Kılıçaslan
emircan@ug.bilkent.edu.tr

To Me

3:36 PM

CTIS496 HW2 Question 2

```
S/MIME Encryption and signed email.
```

Message Security - OpenPGP

Good Digital Signature

This message includes a valid digital signature from a key that you have already accepted. However, you have not yet verified that the key is really owned by the sender.

Signer key ID: 0xD2039FC3427FCB6C

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption ensures the message can only be read by the recipients it was intended for.

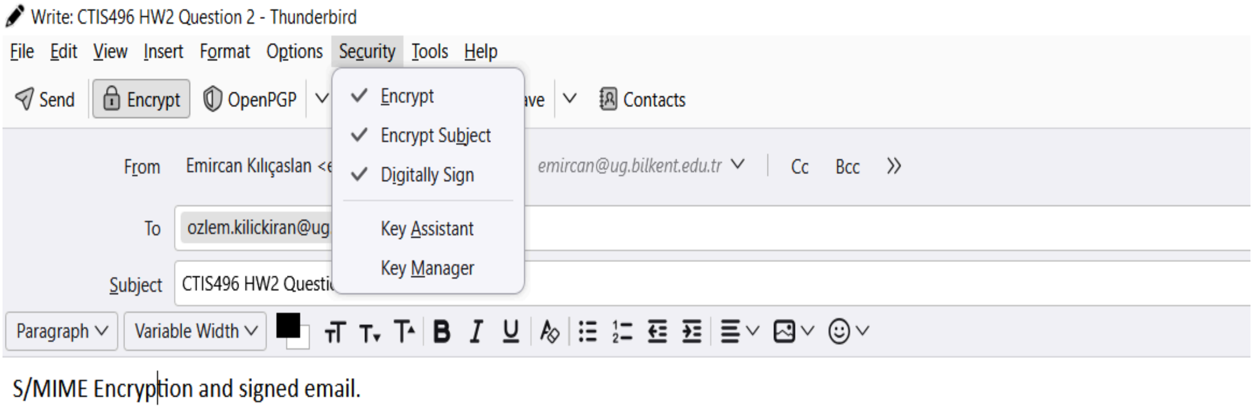
Your decryption key ID: 0x8EC9DCDFE2870339 (Sub key ID: 0x71402ED459BC434F)

In addition, the message was encrypted to the owners of the following keys:

Emircan Kılıçaslan <emircan@ug.bilkent.edu.tr>
0xD2039FC3427FCB6C (0xCB960D3418E67BE8)

1 attachment: OpenPGP_0xD2039FC3427FCB6C.asc 3.1 KB

Emircan’s email sending screen on Thunderbird:



Write: CTIS496 HW2 Question 2 - Thunderbird

Security:
- ✓ Encrypt
- ✓ Encrypt Subject
- ✓ Digitally Sign

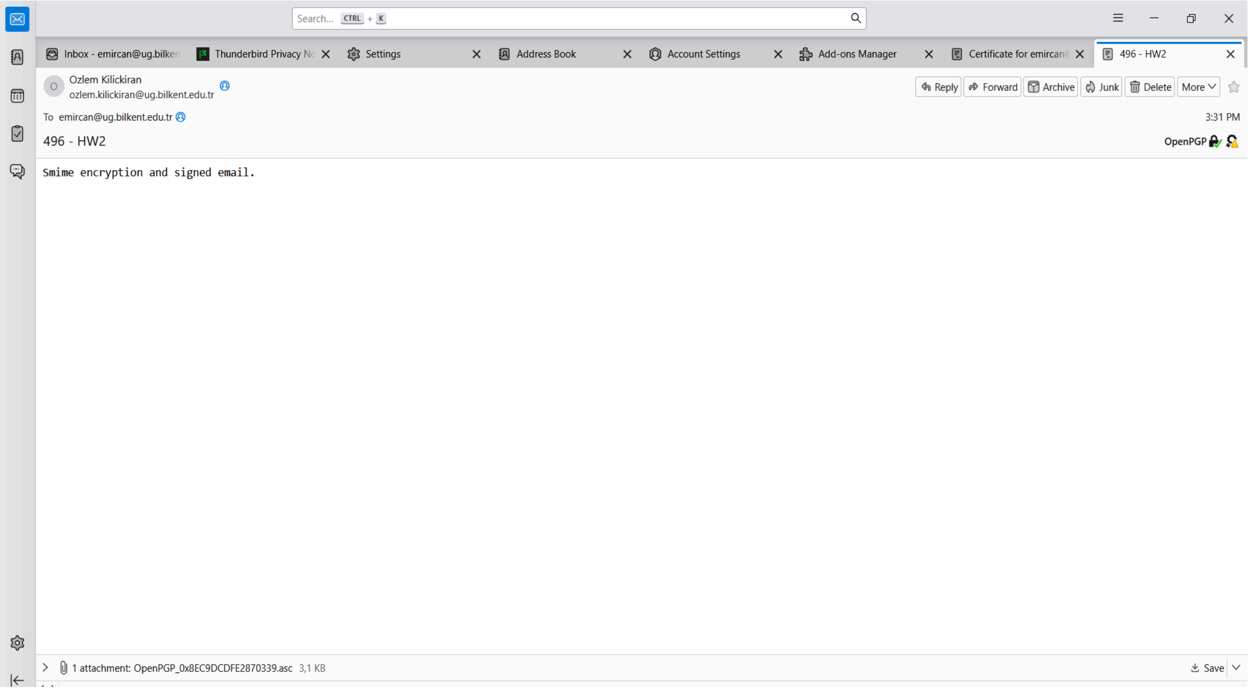
From Emircan Kılıçaslan <e ... emircan@ug.bilkent.edu.tr

To ozlem.kilickiran@ug

Subject CTIS496 HW2 Questi

S/MIME Encryption and signed email.

Emircan’s screen showing Emircan’s email on Thunderbird:



Ozlem Kilickiran
ozlem.kilickiran@ug.bilkent.edu.tr

To emircan@ug.bilkent.edu.tr

3:31 PM

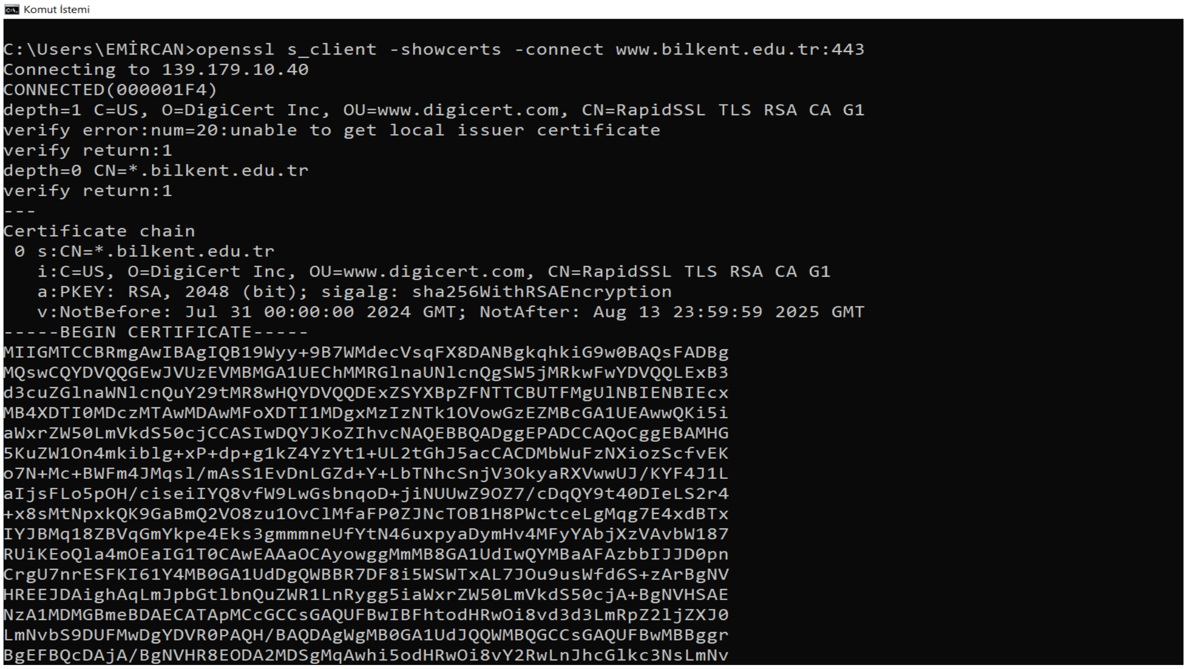
496 - HW2

```
Smime encryption and signed email.
```

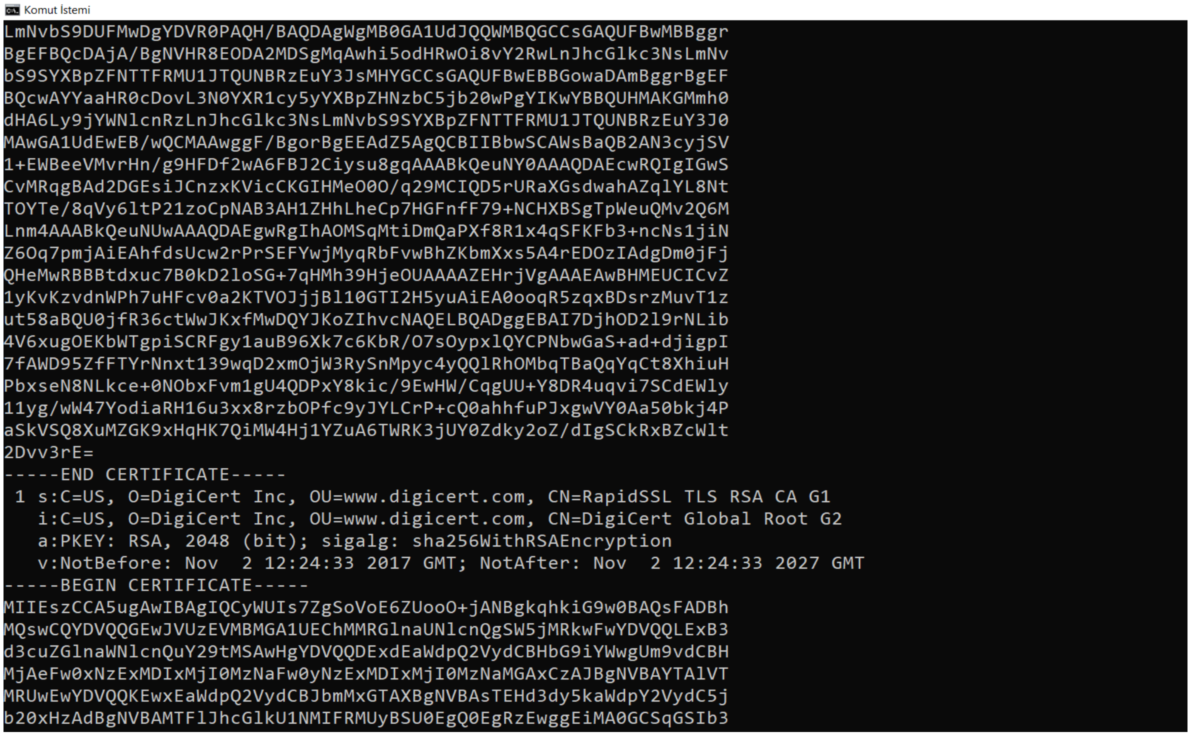
1 attachment: OpenPGP_0x8EC9DCDFE2870339.asc 3,1 KB

Q3-

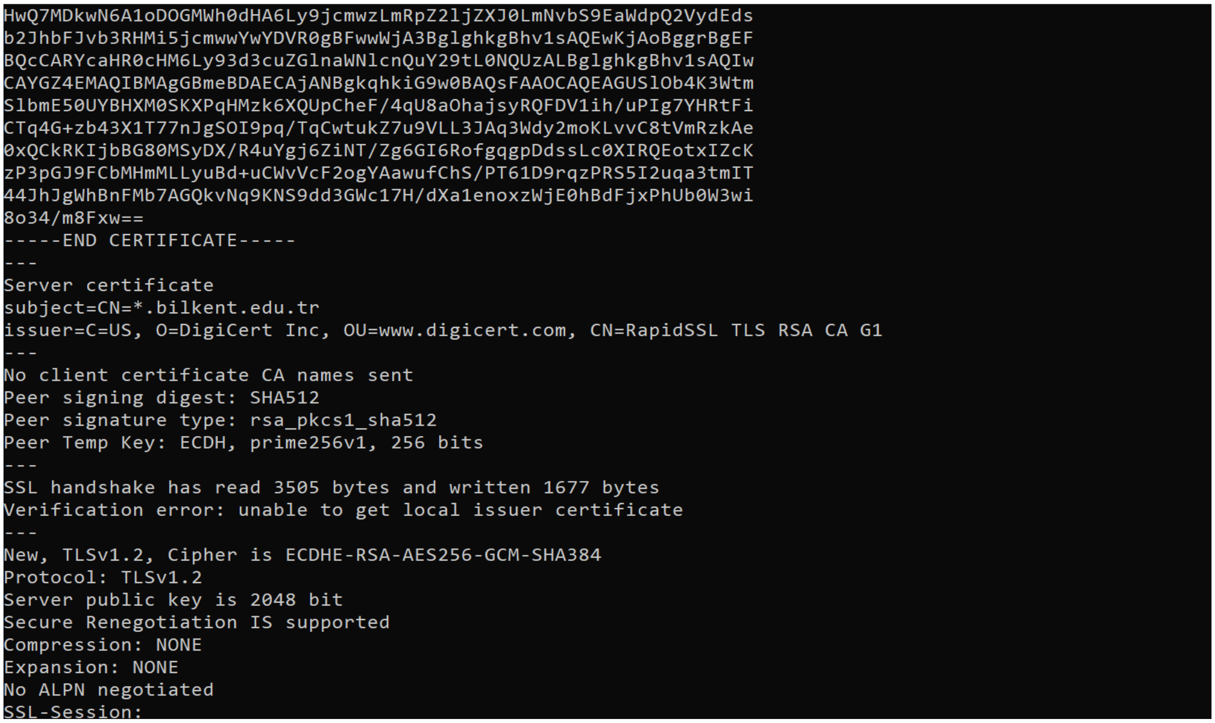
Emircan’s Screen



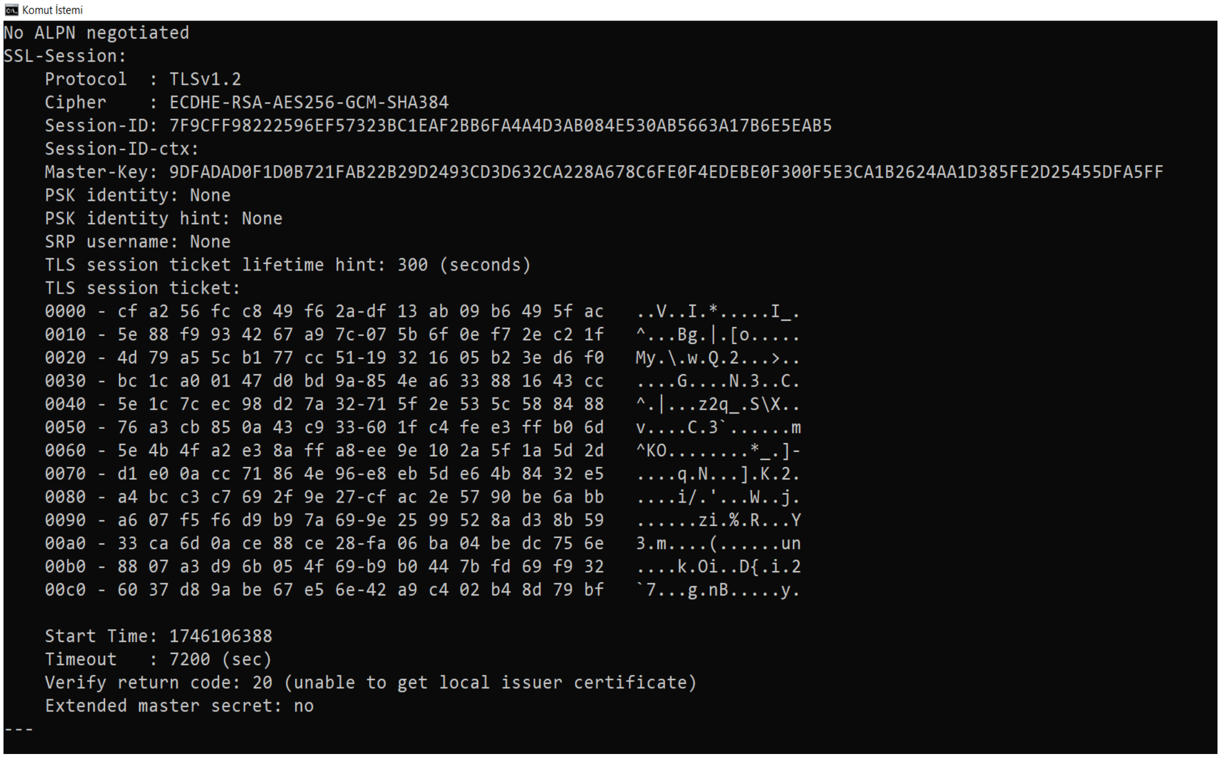
```
C:\Users\EMİRCAN>openssl s_client -showcerts -connect www.bilkent.edu.tr:443
Connecting to 139.179.10.40
CONNECTED(000001F4)
depth=1 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=*.bilkent.edu.tr
verify return:1
---
Certificate chain
 0 s:CN=*.bilkent.edu.tr
   i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Jul 31 00:00:00 2024 GMT; NotAfter: Aug 13 23:59:59 2025 GMT
-----BEGIN CERTIFICATE-----
MIIGMTCCBRmgAwIBAgIQB19Wyy+9B7WMdecVsqFX8DANBgkqhkiG9w0BAQsFADBg
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMR8wHQYDVQQDExZSYXBpZFNTTCBUTFMgUlNBIENBIEcx
MB4XDTI0MDczMTAwMDAwMFoXDTI1MDgxMzIzNTk1OVowGzEZMBcGA1UEAwwQKi5i
aWxrZW50LmVkdS50cjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMHG
5KuZW1On4mkiblg+xP+dp+g1kZ4YzYt1+UL2tGhJ5acCACDMbWuFzNXiozScfvEK
o7N+Mc+BWFm4JMqsl/mAsS1EvDnLGZd+Y+LbTNhcSnjV3OkyaRXVwwUJ/KYF4J1L
aIjsFLo5pOH/ciseiIYQ8vfW9LwGsbnqoD+jiNUUwZ9OZ7/cDqQY9t40DIeLS2r4
+x8sMtNpxkQK9GaBmQ2VO8zu1OvClMfaFP0ZJNcTOB1H8PWctceLgMqg7E4xdBTx
IYJBMq18ZBVqGmYkpe4Eks3gmmmneUfYtN46uxpyaDymHv4MFyYAbjXzVAvbW187
RUiKEoQla4mOEaIG1T0CAwEAAaOCAyowggMmMB8GA1UdIwQYMBaAFAzbbIJJD0pn
CrgU7nrESFKI61Y4MB0GA1UdDgQWBBR7DF8i5WSWTxAL7JOu9usWfd6S+zArBgNV
HREEJDAighAqLmJpbGtlbnQuZWR1LnRygg5iaWxrZW50LmVkdS50cjA+BgNVHSAE
NzA1MDMGBmeBDAECATApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2ljZXJ0
LmNvbS9DUFMwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjA/BgNVHR8EODA2MDSgMqAwhi5odHRwOi8vY2RwLnJhcGlkc3NsLmNv
```



```
LmNvbS9DUFMwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjA/BgNVHR8EODA2MDSgMqAwhi5odHRwOi8vY2RwLnJhcGlkc3NsLmNv
bS9SYXBpZFNTTFRMU1JTQUNBRzEuY3JsMHYGCCsGAQUFBwEBBGowaDAmBggrBgEF
BQcwAYYaaHR0cDovL3N0YXR1cy5yYXBpZHNzbC5jb20wPgYIKwYBBQUHMAKGMmh0
dHA6Ly9jYWNlcnRzLnJhcGlkc3NsLmNvbS9SYXBpZFNTTFRMU1JTQUNBRzEuY3J0
MAwGA1UdEwEB/wQCMAAwggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB2AN3cyjSV
1+EWBeeVMvrHn/g9HFDf2wA6FBJ2Ciysu8gqAAABkQeuNY0AAAQDAEcwRQIgIGwS
CvMRqgBAd2DGEsiJCnzxKVicCKGIHMeO0O/q29MCIQD5rURaXGsdwahAZqlYL8Nt
TOYTe/8qVy6ltP21zoCpNAB3AH1ZHhLheCp7HGFnfF79+NCHXBSgTpWeuQMv2Q6M
Lnm4AAABkQeuNUwAAAQDAEgwRgIhAOMSqMtiDmQaPXf8R1x4qSFKFb3+ncNs1jiN
Z6Oq7pmjAiEAhfdsUcw2rPrSEFYwjMyqRbFvwBhZKbmXxs5A4rEDOzIAdgDm0jFj
QHeMwRBBBtdxuc7B0kD2loSG+7qHMh39HjeOUAAAAZEHrjVgAAAEAwBHMEUCICvZ
1yKvKzvdnWPh7uHFcv0a2KTVOJjjBl10GTI2H5yuAiEA0ooqR5zqxBDsrzMuvT1z
ut58aBQU0jfR36ctWwJKxfMwDQYJKoZIhvcNAQELBQADggEBAI7DjhOD2l9rNLib
4V6xugOEKbWTgpiSCRFgy1auB96Xk7c6KbR/O7sOypxlQYCPNbwGaS+ad+djigpI
7fAWD95ZfFTYrNnxt139wqD2xmOjW3RySnMpyc4yQQlRhOMbqTBaQqYqCt8XhiuH
PbxseN8NLkce+0NObxFvm1gU4QDPxY8kic/9EwHW/CqgUU+Y8DR4uqvi7SCdEWly
11yg/wW47YodiaRH16u3xx8rzbOPfc9yJYLCrP+cQ0ahhfuPJxgwVY0Aa50bkj4P
aSkVSQ8XuMZGK9xHqHK7QiMW4Hj1YZuA6TWRK3jUY0Zdky2oZ/dIgSCkRxBZcWlt
2Dvv3rE=
-----END CERTIFICATE-----
 1 s:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
   i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G2
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Nov  2 12:24:33 2017 GMT; NotAfter: Nov  2 12:24:33 2027 GMT
-----BEGIN CERTIFICATE-----
MIIEszCCA5ugAwIBAgIQCyWUIs7ZgSoVoE6ZUooO+jANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xNzExMDIxMjI0MzNaFw0yNzExMDIxMjI0MzNaMGAxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xHzAdBgNVBAMTFlJhcGlkU1NMIFRMUyBSU0EgQ0EgRzEwggEiMA0GCSqGSIb3
```

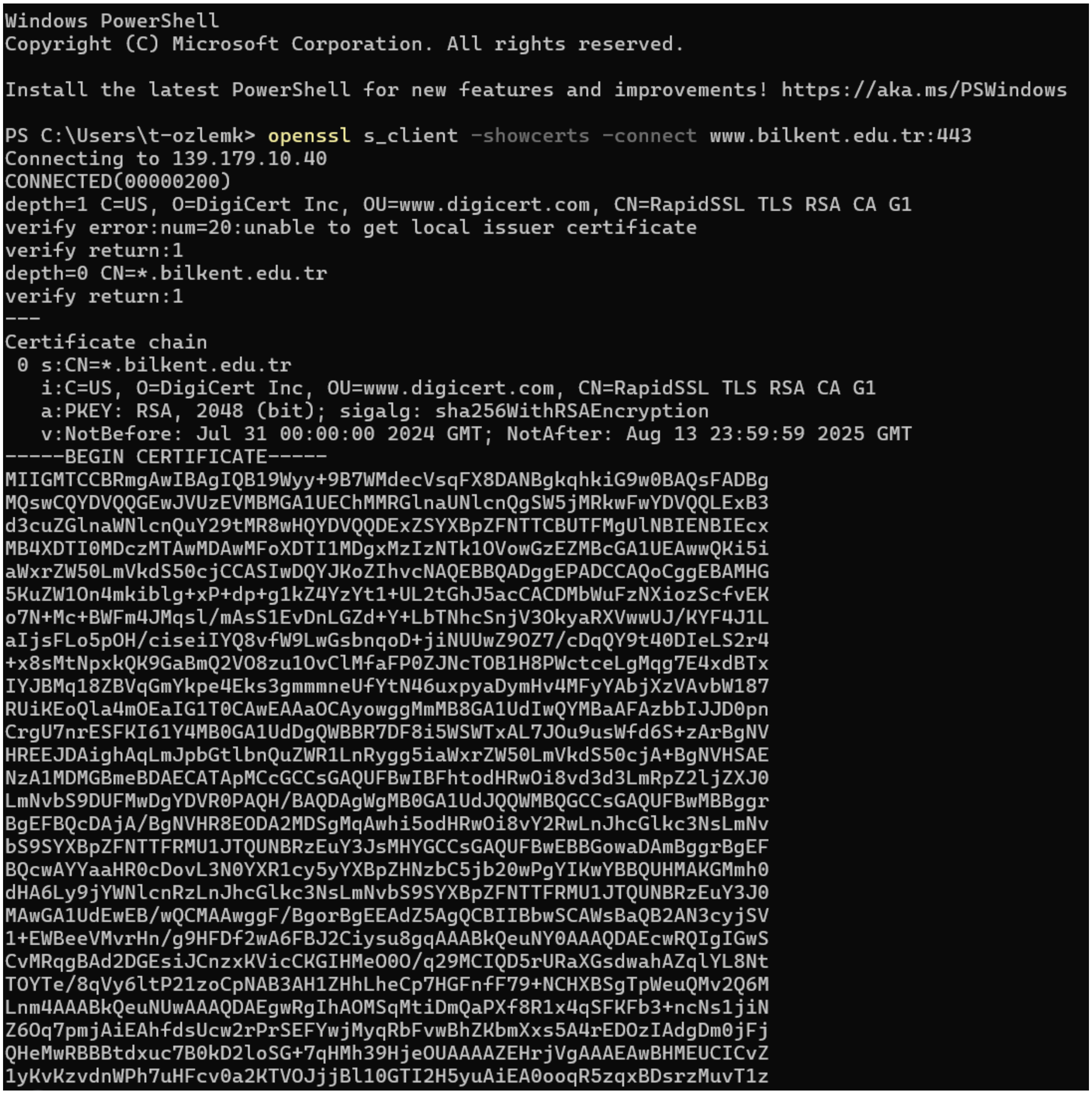


```
HwQ7MDkwN6A1oDOGMWh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEds
b2JhbFJvb3RHMi5jcmwwYwYDVR0gBFwwWjA3BglghkgBhv1sAQEwKjAoBggrBgEF
BQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzALBglghkgBhv1sAQIw
CAYGZ4EMAQIBMAgGBmeBDAECAjANBgkqhkiG9w0BAQsFAAOCAQEAGUSlOb4K3Wtm
SlbmE50UYBHXM0SKXPqHMzk6XQUpCheF/4qU8aOhajsyRQFDV1ih/uPIg7YHRtFi
CTq4G+zb43X1T77nJgSOI9pq/TqCwtukZ7u9VLL3JAq3Wdy2moKLvvC8tVmRzkAe
0xQCkRKIjbBG80MSyDX/R4uYgj6ZiNT/Zg6GI6RofgqgpDdssLc0XIRQEotxIZcK
zP3pGJ9FCbMHmMLLyuBd+uCWvVcF2ogYAawufChS/PT61D9rqzPRS5I2uqa3tmIT
44JhJgWhBnFMb7AGQkvNq9KNS9dd3GWc17H/dXa1enoxzWjE0hBdFjxPhUb0W3wi
8o34/m8Fxw==
-----END CERTIFICATE-----
---
Server certificate
subject=CN=*.bilkent.edu.tr
issuer=C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
---
No client certificate CA names sent
Peer signing digest: SHA512
Peer signature type: rsa_pkcs1_sha512
Peer Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 3505 bytes and written 1677 bytes
Verification error: unable to get local issuer certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Protocol: TLSv1.2
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
```

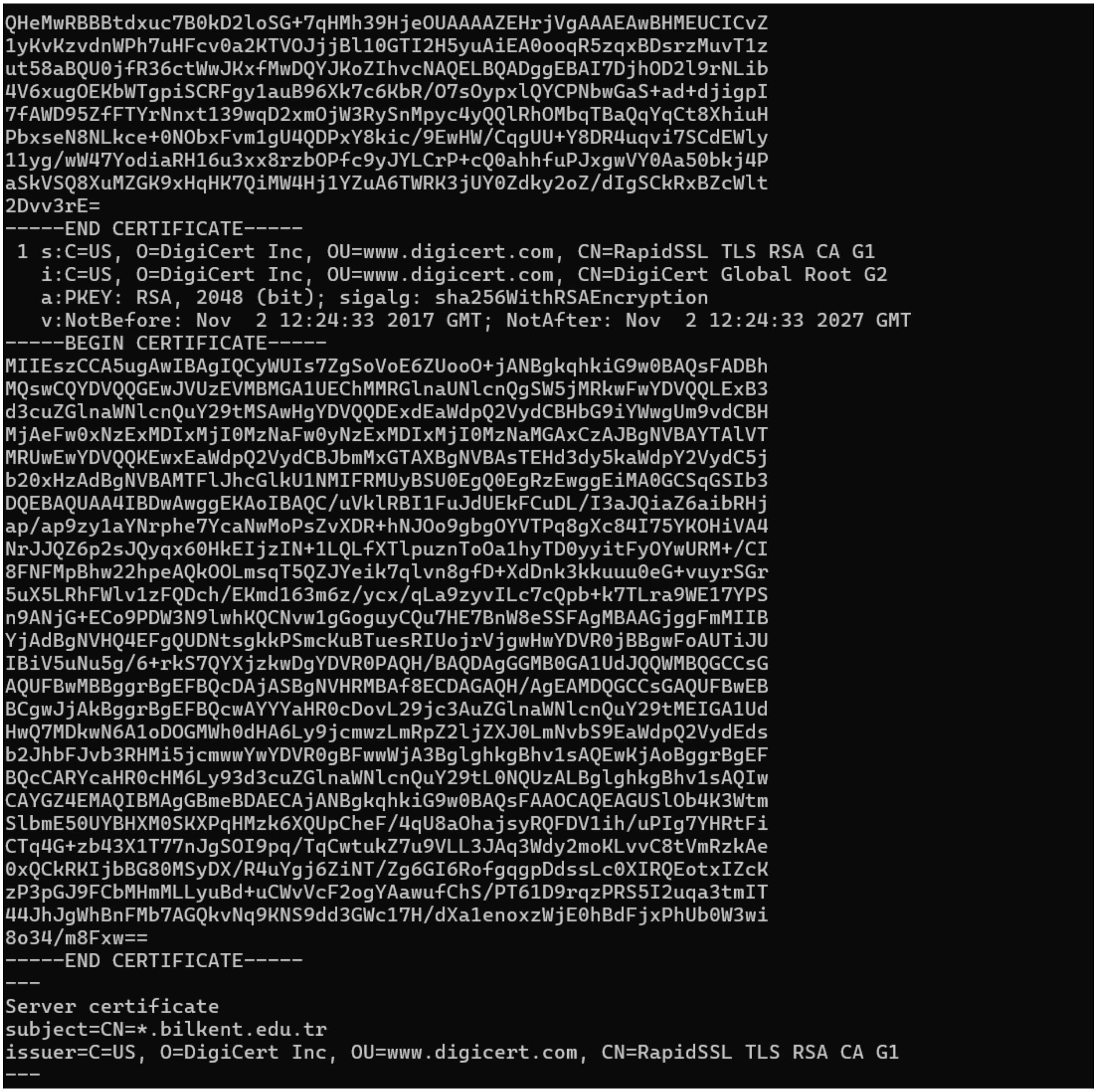


```
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 7F9CFF98222596EF57323BC1EAF2BB6FA4A4D3AB084E530AB5663A17B6E5EAB5
    Session-ID-ctx:
    Master-Key: 9DFADAD0F1D0B721FAB22B29D2493CD3D632CA228A678C6FE0F4EDEBE0F300F5E3CA1B2624AA1D385FE2D25455DFA5FF
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - cf a2 56 fc c8 49 f6 2a-df 13 ab 09 b6 49 5f ac   ..V..I.*.....I_.
    0010 - 5e 88 f9 93 42 67 a9 7c-07 5b 6f 0e f7 2e c2 1f   ^...Bg.|.[o.....
    0020 - 4d 79 a5 5c b1 77 cc 51-19 32 16 05 b2 3e d6 f0   My.\.w.Q.2...>..
    0030 - bc 1c a0 01 47 d0 bd 9a-85 4e a6 33 88 16 43 cc   ....G....N.3..C.
    0040 - 5e 1c 7c ec 98 d2 7a 32-71 5f 2e 53 5c 58 84 88   ^.|...z2q_.S\X..
    0050 - 76 a3 cb 85 0a 43 c9 33-60 1f c4 fe e3 ff b0 6d   v....C.3`......m
    0060 - 5e 4b 4f a2 e3 8a ff a8-ee 9e 10 2a 5f 1a 5d 2d   ^KO........*_.]-
    0070 - d1 e0 0a cc 71 86 4e 96-e8 eb 5d e6 4b 84 32 e5   ....q.N...].K.2.
    0080 - a4 bc c3 c7 69 2f 9e 27-cf ac 2e 57 90 be 6a bb   ....i/.'...W..j.
    0090 - a6 07 f5 f6 d9 b9 7a 69-9e 25 99 52 8a d3 8b 59   ......zi.%.R...Y
    00a0 - 33 ca 6d 0a ce 88 ce 28-fa 06 ba 04 be dc 75 6e   3.m....(......un
    00b0 - 88 07 a3 d9 6b 05 4f 69-b9 b0 44 7b fd 69 f9 32   ....k.Oi..D{.i.2
    00c0 - 60 37 d8 9a be 67 e5 6e-42 a9 c4 02 b4 8d 79 bf   `7...g.nB.....y.

    Start Time: 1746106388
    Timeout   : 7200 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
    Extended master secret: no
---
```

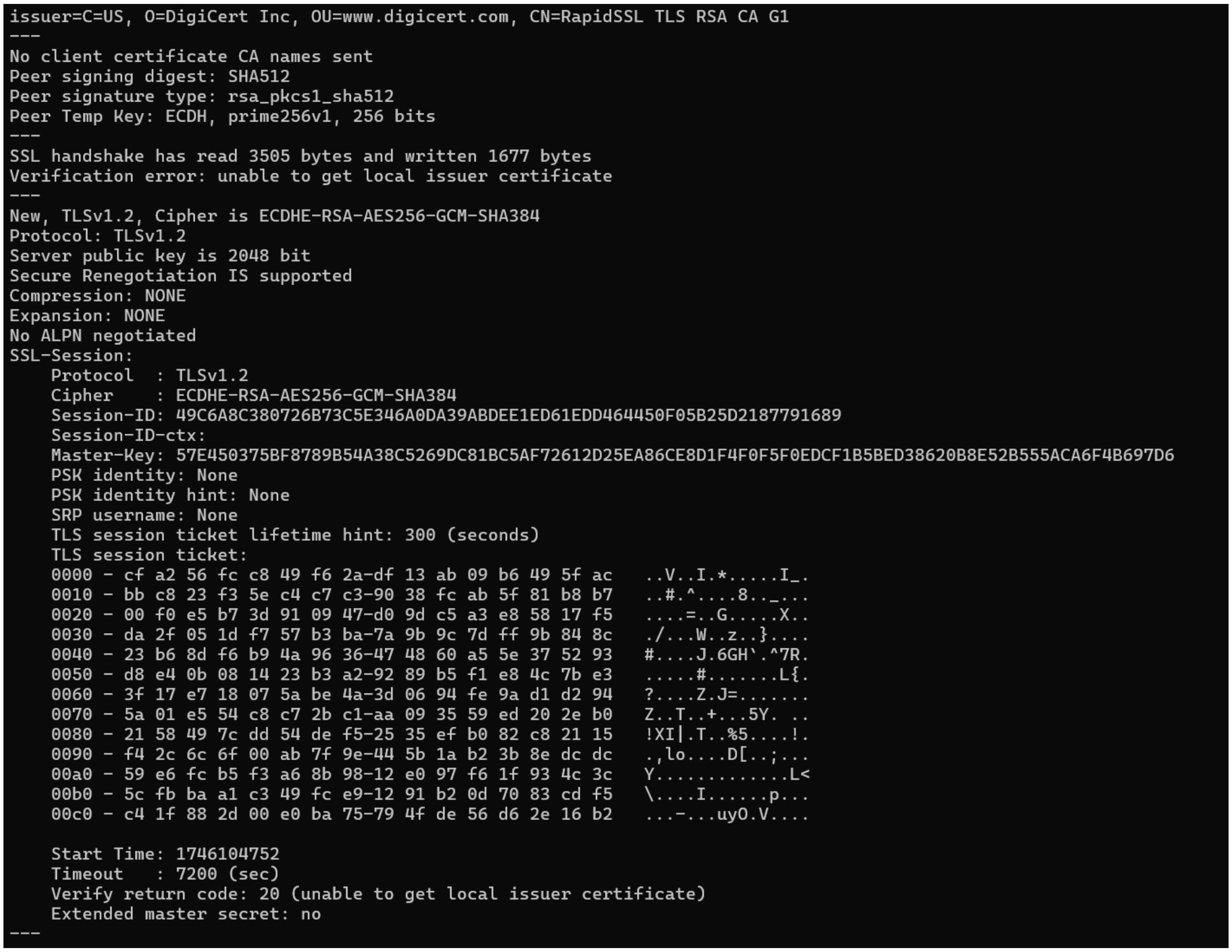
Özlem’s Screen:



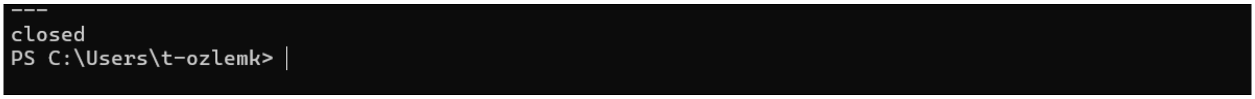
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\t-ozlemk> openssl s_client -showcerts -connect www.bilkent.edu.tr:443
Connecting to 139.179.10.40
CONNECTED(00000200)
depth=1 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=*.bilkent.edu.tr
verify return:1
---
Certificate chain
 0 s:CN=*.bilkent.edu.tr
   i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Jul 31 00:00:00 2024 GMT; NotAfter: Aug 13 23:59:59 2025 GMT
-----BEGIN CERTIFICATE-----
MIIGMTCCBRmgAwIBAgIQB19Wyy+9B7WMdecVsqFX8DANBgkqhkiG9w0BAQsFADBg
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMR8wHQYDVQQDExZSYXBpZFNTTCBUTFMgUlNBIENBIEcx
MB4XDTI0MDczMTAwMDAwMFoXDTI1MDgxMzIzNTk1OVowGzEZMBcGA1UEAwwQKi5i
aWxrZW50LmVkdS50cjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMHG
5KuZW1On4mkiblg+xP+dp+g1kZ4YzYt1+UL2tGhJ5acCACDMbWuFzNXiozScfvEK
o7N+Mc+BWFm4JMqsl/mAsS1EvDnLGZd+Y+LbTNhcSnjV3OkyaRXVwwUJ/KYF4J1L
aIjsFLo5pOH/ciseiIYQ8vfW9LwGsbnqoD+jiNUUwZ9OZ7/cDqQY9t40DIeLS2r4
+x8sMtNpxkQK9GaBmQ2VO8zu1OvClMfaFP0ZJNcTOB1H8PWctceLgMqg7E4xdBTx
IYJBMq18ZBVqGmYkpe4Eks3gmmmneUfYtN46uxpyaDymHv4MFyYAbjXzVAvbW187
RUiKEoQla4mOEaIG1T0CAwEAAaOCAyowggMmMB8GA1UdIwQYMBaAFAzbbIJJD0pn
CrgU7nrESFKI61Y4MB0GA1UdDgQWBBR7DF8i5WSWTxAL7JOu9usWfd6S+zArBgNV
HREEJDAighAqLmJpbGtlbnQuZWR1LnRygg5iaWxrZW50LmVkdS50cjA+BgNVHSAE
NzA1MDMGBmeBDAECATApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2ljZXJ0
LmNvbS9DUFMwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjA/BgNVHR8EODA2MDSgMqAwhi5odHRwOi8vY2RwLnJhcGlkc3NsLmNv
bS9SYXBpZFNTTFRMU1JTQUNBRzEuY3JsMHYGCCsGAQUFBwEBBGowaDAmBggrBgEF
BQcwAYYaaHR0cDovL3N0YXR1cy5yYXBpZHNzbC5jb20wPgYIKwYBBQUHMAKGMmh0
dHA6Ly9jYWNlcnRzLnJhcGlkc3NsLmNvbS9SYXBpZFNTTFRMU1JTQUNBRzEuY3J0
MAwGA1UdEwEB/wQCMAAwggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB2AN3cyjSV
1+EWBeeVMvrHn/g9HFDf2wA6FBJ2Ciysu8gqAAABkQeuNY0AAAQDAEcwRQIgIGwS
CvMRqgBAd2DGEsiJCnzxKVicCKGIHMeO0O/q29MCIQD5rURaXGsdwahAZqlYL8Nt
TOYTe/8qVy6ltP21zoCpNAB3AH1ZHhLheCp7HGFnfF79+NCHXBSgTpWeuQMv2Q6M
Lnm4AAABkQeuNUwAAAQDAEgwRgIhAOMSqMtiDmQaPXf8R1x4qSFKFb3+ncNs1jiN
Z6Oq7pmjAiEAhfdsUcw2rPrSEFYwjMyqRbFvwBhZKbmXxs5A4rEDOzIAdgDm0jFj
QHeMwRBBBtdxuc7B0kD2loSG+7qHMh39HjeOUAAAAZEHrjVgAAAEAwBHMEUCICvZ
1yKvKzvdnWPh7uHFcv0a2KTVOJjjBl10GTI2H5yuAiEA0ooqR5zqxBDsrzMuvT1z
```



```
QHeMwRBBBtdxuc7B0kD2loSG+7qHMh39HjeOUAAAAZEHrjVgAAAEAwBHMEUCICvZ
1yKvKzvdnWPh7uHFcv0a2KTVOJjjBl10GTI2H5yuAiEA0ooqR5zqxBDsrzMuvT1z
ut58aBQU0jfR36ctWwJKxfMwDQYJKoZIhvcNAQELBQADggEBAI7DjhOD2l9rNLib
4V6xugOEKbWTgpiSCRFgy1auB96Xk7c6KbR/O7sOypxlQYCPNbwGaS+ad+djigpI
7fAWD95ZfFTYrNnxt139wqD2xmOjW3RySnMpyc4yQQlRhOMbqTBaQqYqCt8XhiuH
PbxseN8NLkce+0NObxFvm1gU4QDPxY8kic/9EwHW/CqgUU+Y8DR4uqvi7SCdEWly
11yg/wW47YodiaRH16u3xx8rzbOPfc9yJYLCrP+cQ0ahhfuPJxgwVY0Aa50bkj4P
aSkVSQ8XuMZGK9xHqHK7QiMW4Hj1YZuA6TWRK3jUY0Zdky2oZ/dIgSCkRxBZcWlt
2Dvv3rE=
-----END CERTIFICATE-----
 1 s:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
   i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root G2
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Nov  2 12:24:33 2017 GMT; NotAfter: Nov  2 12:24:33 2027 GMT
-----BEGIN CERTIFICATE-----
MIIEszCCA5ugAwIBAgIQCyWUIs7ZgSoVoE6ZUooO+jANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xNzExMDIxMjI0MzNaFw0yNzExMDIxMjI0MzNaMGAxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xHzAdBgNVBAMTFlJhcGlkU1NMIFRMUyBSU0EgQ0EgRzEwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC/uVklRBI1FuJdUEkFCuDL/I3aJQiaZ6aibRHj
ap/ap9zy1aYNrphe7YcaNwMoPsZvXDR+hNJOo9gbgOYVTPq8gXc84I75YKOHiVA4
NrJJQZ6p2sJQyqx60HkEIjzIN+1LQLfXTlpuznToOa1hyTD0yyitFyOYwURM+/CI
8FNFMpBhw22hpeAQkOOLmsqT5QZJYeik7qlvn8gfD+XdDnk3kkuuu0eG+vuyrSGr
5uX5LRhFWlv1zFQDch/EKmd163m6z/ycx/qLa9zyvILc7cQpb+k7TLra9WE17YPS
n9ANjG+ECo9PDW3N9lwhKQCNvw1gGoguyCQu7HE7BnW8eSSFAgMBAAGjggFmMIIB
YjAdBgNVHQ4EFgQUDNtsgkkPSmcKuBTuesRIUojrVjgwHwYDVR0jBBgwFoAUTiJU
IBiV5uNu5g/6+rkS7QYXjzkwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjASBgNVHRMBAf8ECDAGAQH/AgEAMDQGCCsGAQUFBwEB
BCgwJjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEIGA1Ud
HwQ7MDkwN6A1oDOGMWh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEds
b2JhbFJvb3RHMi5jcmwwYwYDVR0gBFwwWjA3BglghkgBhv1sAQEwKjAoBggrBgEF
BQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzALBglghkgBhv1sAQIw
CAYGZ4EMAQIBMAgGBmeBDAECAjANBgkqhkiG9w0BAQsFAAOCAQEAGUSlOb4K3Wtm
SlbmE50UYBHXM0SKXPqHMzk6XQUpCheF/4qU8aOhajsyRQFDV1ih/uPIg7YHRtFi
CTq4G+zb43X1T77nJgSOI9pq/TqCwtukZ7u9VLL3JAq3Wdy2moKLvvC8tVmRzkAe
0xQCkRKIjbBG80MSyDX/R4uYgj6ZiNT/Zg6GI6RofgqgpDdssLc0XIRQEotxIZcK
zP3pGJ9FCbMHmMLLyuBd+uCWvVcF2ogYAawufChS/PT61D9rqzPRS5I2uqa3tmIT
44JhJgWhBnFMb7AGQkvNq9KNS9dd3GWc17H/dXa1enoxzWjE0hBdFjxPhUb0W3wi
8o34/m8Fxw==
-----END CERTIFICATE-----
---
Server certificate
subject=CN=*.bilkent.edu.tr
issuer=C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
---
```



```
issuer=C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
---
No client certificate CA names sent
Peer signing digest: SHA512
Peer signature type: rsa_pkcs1_sha512
Peer Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 3505 bytes and written 1677 bytes
Verification error: unable to get local issuer certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Protocol: TLSv1.2
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 49C6A8C380726B73C5E346A0DA39ABDEE1ED61EDD464450F05B25D2187791689
    Session-ID-ctx:
    Master-Key: 57E450375BF8789B54A38C5269DC81BC5AF72612D25EA86CE8D1F4F0F5F0EDCF1B5BED38620B8E52B555ACA6F4B697D6
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - cf a2 56 fc c8 49 f6 2a-df 13 ab 09 b6 49 5f ac   ..V..I.*.....I_.
    0010 - bb c8 23 f3 5e c4 c7 c3-90 38 fc ab 5f 81 b8 b7   ..#.^....8.._...
    0020 - 00 f0 e5 b7 3d 91 09 47-d0 9d c5 a3 e8 58 17 f5   ....=..G.....X..
    0030 - da 2f 05 1d f7 57 b3 ba-7a 9b 9c 7d ff 9b 84 8c   ./...W..z..}....
    0040 - 23 b6 8d f6 b9 4a 96 36-47 48 60 a5 5e 37 52 93   #....J.6GH`.^7R.
    0050 - d8 e4 0b 08 14 23 b3 a2-92 89 b5 f1 e8 4c 7b e3   .....#.......L{.
    0060 - 3f 17 e7 18 07 5a be 4a-3d 06 94 fe 9a d1 d2 94   ?....Z.J=.......
    0070 - 5a 01 e5 54 c8 c7 2b c1-aa 09 35 59 ed 20 2e b0   Z..T..+...5Y. ..
    0080 - 21 58 49 7c dd 54 de f5-25 35 ef b0 82 c8 21 15   !XI|.T..%5....!.
    0090 - f4 2c 6c 6f 00 ab 7f 9e-44 5b 1a b2 3b 8e dc dc   .,lo....D[..;...
    00a0 - 59 e6 fc b5 f3 a6 8b 98-12 e0 97 f6 1f 93 4c 3c   Y.............L<
    00b0 - 5c fb ba a1 c3 49 fc e9-12 91 b2 0d 70 83 cd f5   \....I......p...
    00c0 - c4 1f 88 2d 00 e0 ba 75-79 4f de 56 d6 2e 16 b2   ...-...uyO.V....

    Start Time: 1746104752
    Timeout   : 7200 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
    Extended master secret: no
---
```



```
---
closed
PS C:\Users\t-ozlemk> |
```

What Is Included in the Output?

The output of `openssl s_client -showcerts -connect www.bilkent.edu.tr:443` includes the full certificate chain, details about the TLS handshake, and the verification result. It shows the PEM-encoded certificates, as well as identifying information such as the certificate subject, issuer, and validity.

Output Section	Description
`CONNECTED(000001AC)`	**Confirms TCP connection to the server was successful**
`Certificate chain`	**Shows all certificates from the server to the root CA**

`-----BEGIN CERTIFICATE-----`	**PEM-formatted certificates used during the TLS handshake**
`subject=`	**The identity of the website (e.g., domain name, organization)**
`issuer=`	**The Certificate Authority (CA) that issued the certificate**
`SSL handshake has read ...`	**Details about bytes read/written during the handshake**
`New, TLSv1.3, Cipher ...`	**The negotiated TLS version and cipher suite**
`Verify return code: 0 (ok)`	**Indicates the certificate is valid and trusted (0 = success)**

Q4-

- We downloaded GlobalSign's CRL from:

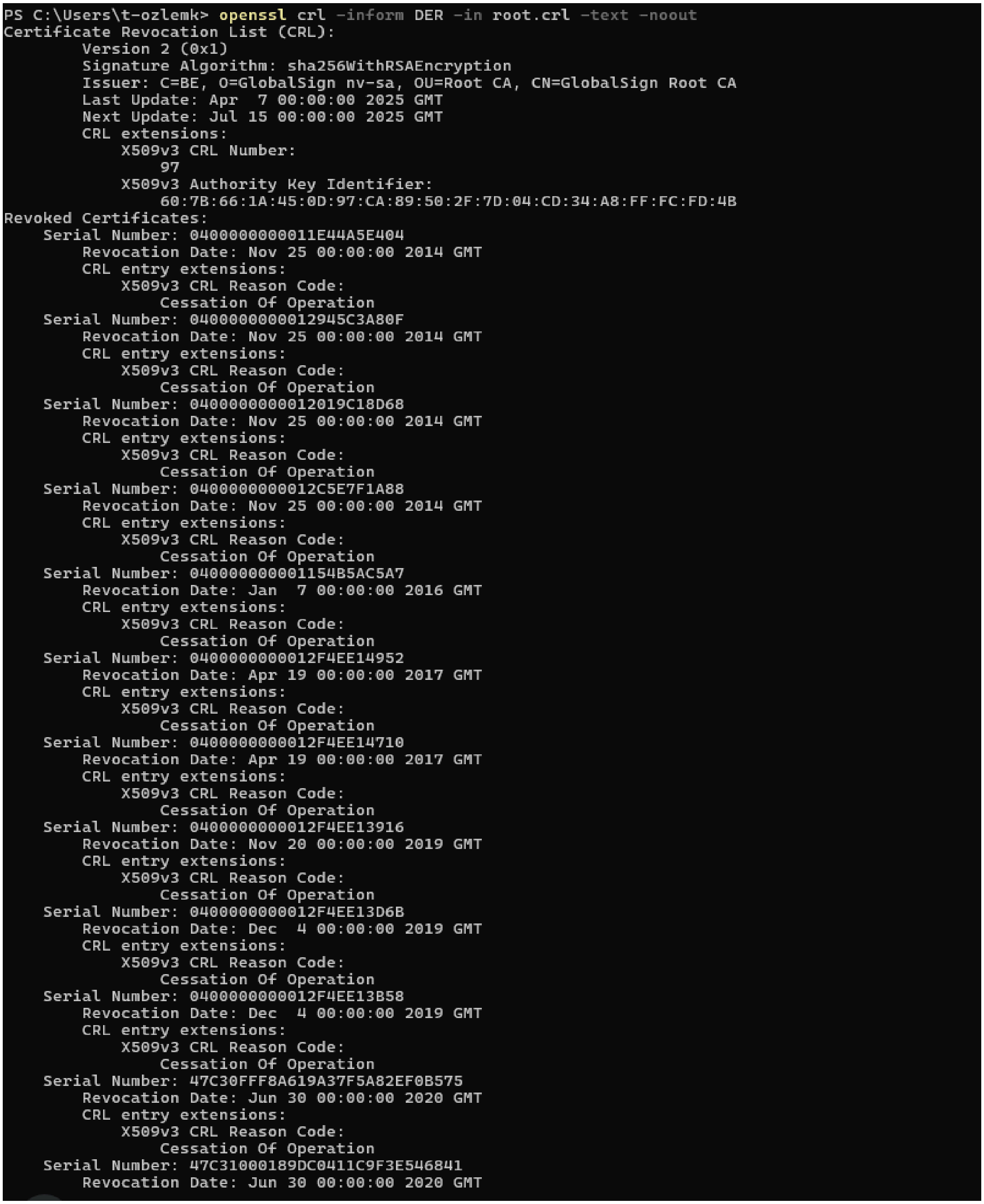
  http://crl.globalsign.net/root.crl

- The following command:

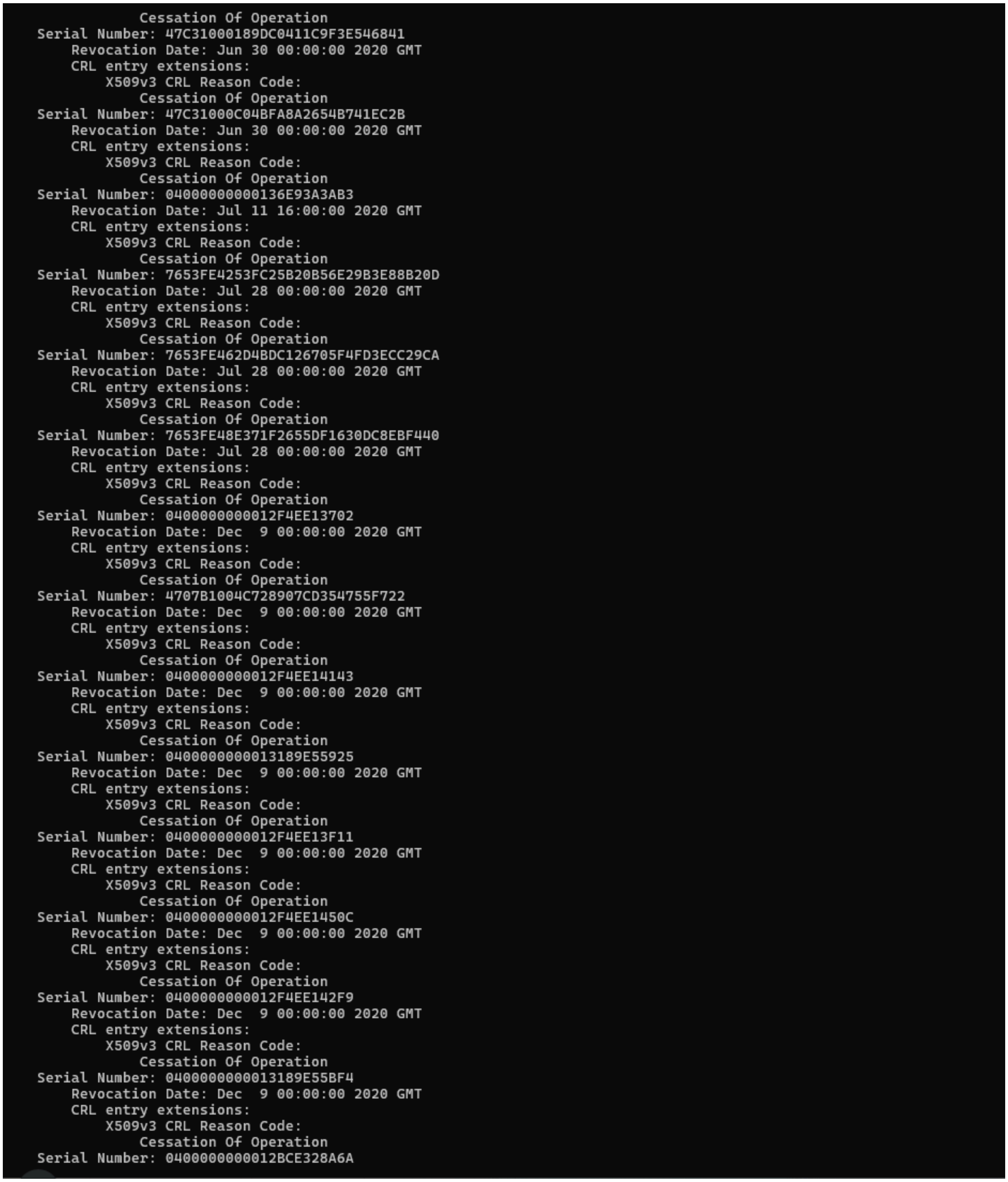
  ```
  openssl crl -inform DER -in root.crl -text -noout
  ```

  will show the **revoked certificates** under `Revoked Certificates`

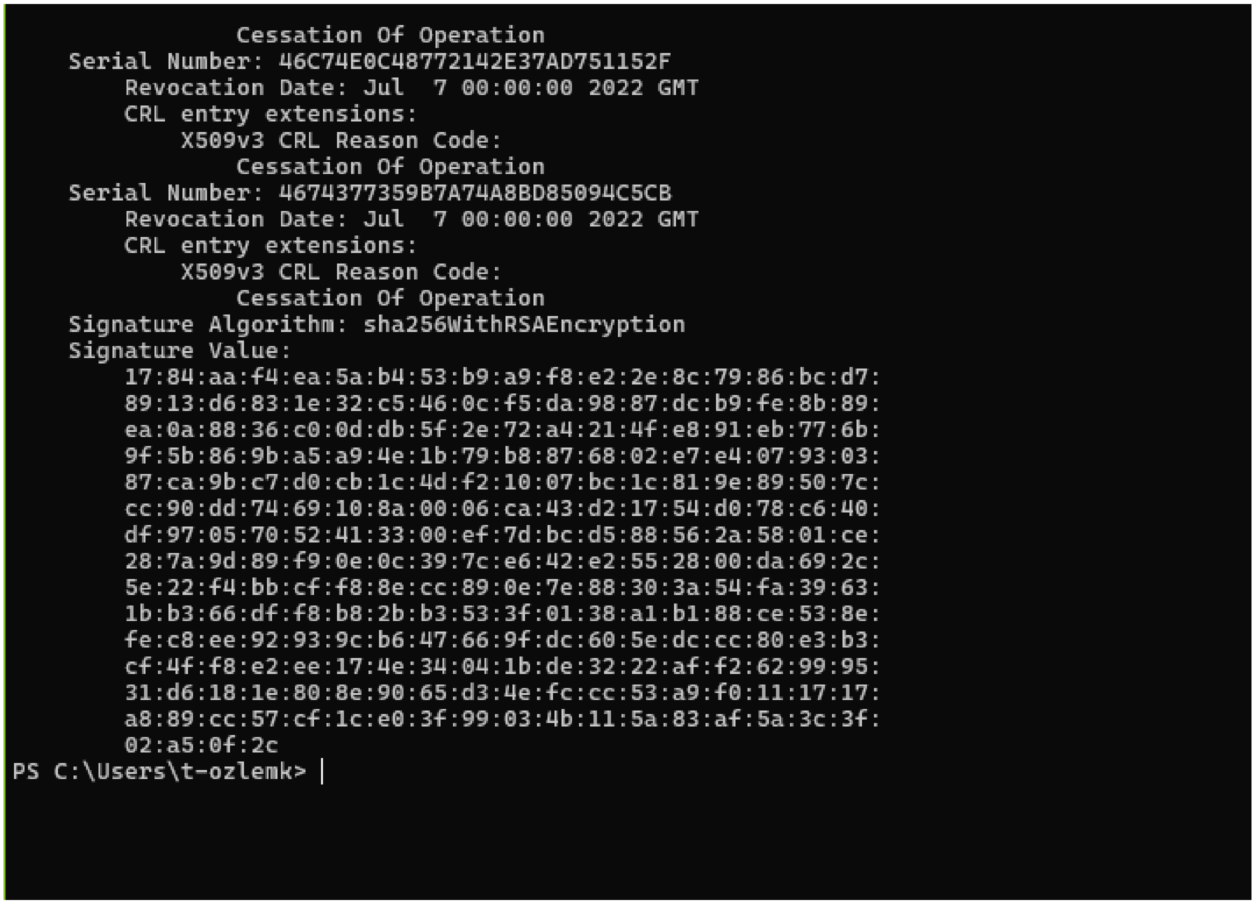
Özlem’s Screen



```
PS C:\Users\t-ozlemk> openssl crl -inform DER -in root.crl -text -noout
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
        Last Update: Apr  7 00:00:00 2025 GMT
        Next Update: Jul 15 00:00:00 2025 GMT
        CRL extensions:
            X509v3 CRL Number:
                97
            X509v3 Authority Key Identifier:
                60:7B:66:1A:45:0D:97:CA:89:50:2F:7D:04:CD:34:A8:FF:FC:FD:4B
Revoked Certificates:
    Serial Number: 0400000000011E44A5E404
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012945C3A80F
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012019C18D68
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012C5E7F1A88
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 04000000001154B5AC5A7
        Revocation Date: Jan  7 00:00:00 2016 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE14952
        Revocation Date: Apr 19 00:00:00 2017 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE14710
        Revocation Date: Apr 19 00:00:00 2017 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE13916
        Revocation Date: Nov 20 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE13D6B
        Revocation Date: Dec  4 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE13B58
        Revocation Date: Dec  4 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 47C30FFF8A619A37F5A82EF0B575
        Revocation Date: Jun 30 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 47C31000189DC0411C9F3E546841
        Revocation Date: Jun 30 00:00:00 2020 GMT
```



```
                Cessation Of Operation
    Serial Number: 47C31000189DC0411C9F3E546841
        Revocation Date: Jun 30 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 47C31000C04BFA8A2654B741EC2B
        Revocation Date: Jun 30 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000136E93A3AB3
        Revocation Date: Jul 11 16:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 7653FE4253FC25B20B56E29B3E88B20D
        Revocation Date: Jul 28 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 7653FE462D4BDC126705F4FD3ECC29CA
        Revocation Date: Jul 28 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 7653FE48E371F2655DF1630DC8EBF440
        Revocation Date: Jul 28 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE13702
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 4707B1004C728907CD354755F722
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE14143
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000013189E55925
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE13F11
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE1450C
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012F4EE142F9
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000013189E55BF4
        Revocation Date: Dec  9 00:00:00 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000012BCE328A6A
```



```
                Cessation Of Operation
    Serial Number: 46C74E0C48772142E37AD751152F
        Revocation Date: Jul  7 00:00:00 2022 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 4674377359B7A74A8BD85094C5CB
        Revocation Date: Jul  7 00:00:00 2022 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        17:84:aa:f4:ea:5a:b4:53:b9:a9:f8:e2:2e:8c:79:86:bc:d7:
        89:13:d6:83:1e:32:c5:46:0c:f5:da:98:87:dc:b9:fe:8b:89:
        ea:0a:88:36:c0:0d:db:5f:2e:72:a4:21:4f:e8:91:eb:77:6b:
        9f:5b:86:9b:a5:a9:4e:1b:79:b8:87:68:02:e7:e4:07:93:03:
        87:ca:9b:c7:d0:cb:1c:4d:f2:10:07:bc:1c:81:9e:89:50:7c:
        cc:90:dd:74:69:10:8a:00:06:ca:43:d2:17:54:d0:78:c6:40:
        df:97:05:70:52:41:33:00:ef:7d:bc:d5:88:56:2a:58:01:ce:
        28:7a:9d:89:f9:0e:0c:39:7c:e6:42:e2:55:28:00:da:69:2c:
        5e:22:f4:bb:cf:f8:8e:cc:89:0e:7e:88:30:3a:54:fa:39:63:
        1b:b3:66:df:f8:b8:2b:b3:53:3f:01:38:a1:b1:88:ce:53:8e:
        fe:c8:ee:92:93:9c:b6:47:66:9f:dc:60:5e:dc:cc:80:e3:b3:
        cf:4f:f8:e2:ee:17:4e:34:04:1b:de:32:22:af:f2:62:99:95:
        31:d6:18:1e:80:8e:90:65:d3:4e:fc:cc:53:a9:f0:11:17:17:
        a8:89:cc:57:cf:1c:e0:3f:99:03:4b:11:5a:83:af:5a:3c:3f:
        02:a5:0f:2c
PS C:\Users\t-ozlemk>
```

Özlem's Answers:

CRL Source

- **CA**: GlobalSign
- **CRL File**: root.crl
- **URL Used**: http://crl.globalsign.net/root.crl

Last Update and Next Update

From your output:

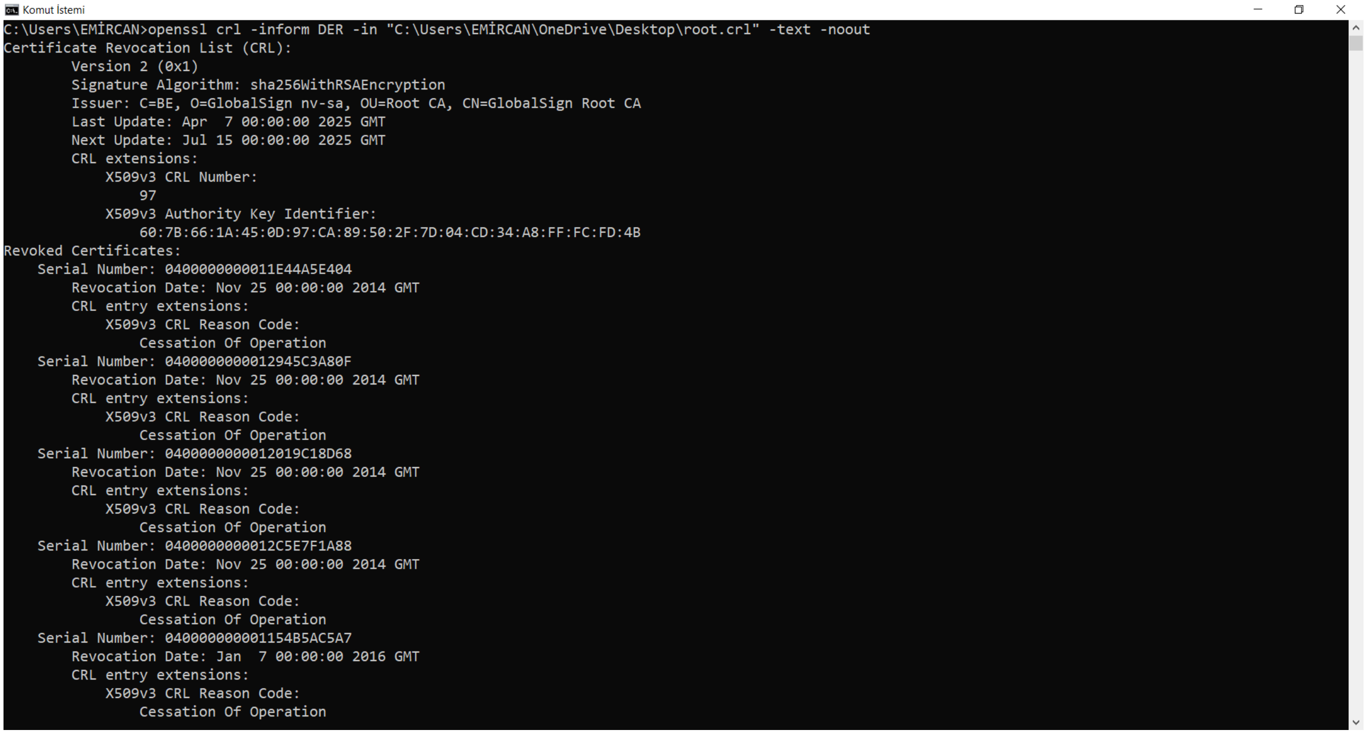
- **Last Update**: Apr 7 00:00:00 2025 GMT
- **Next Update**: Jul 15 00:00:00 2025 GMT

Two Revoked Certificates

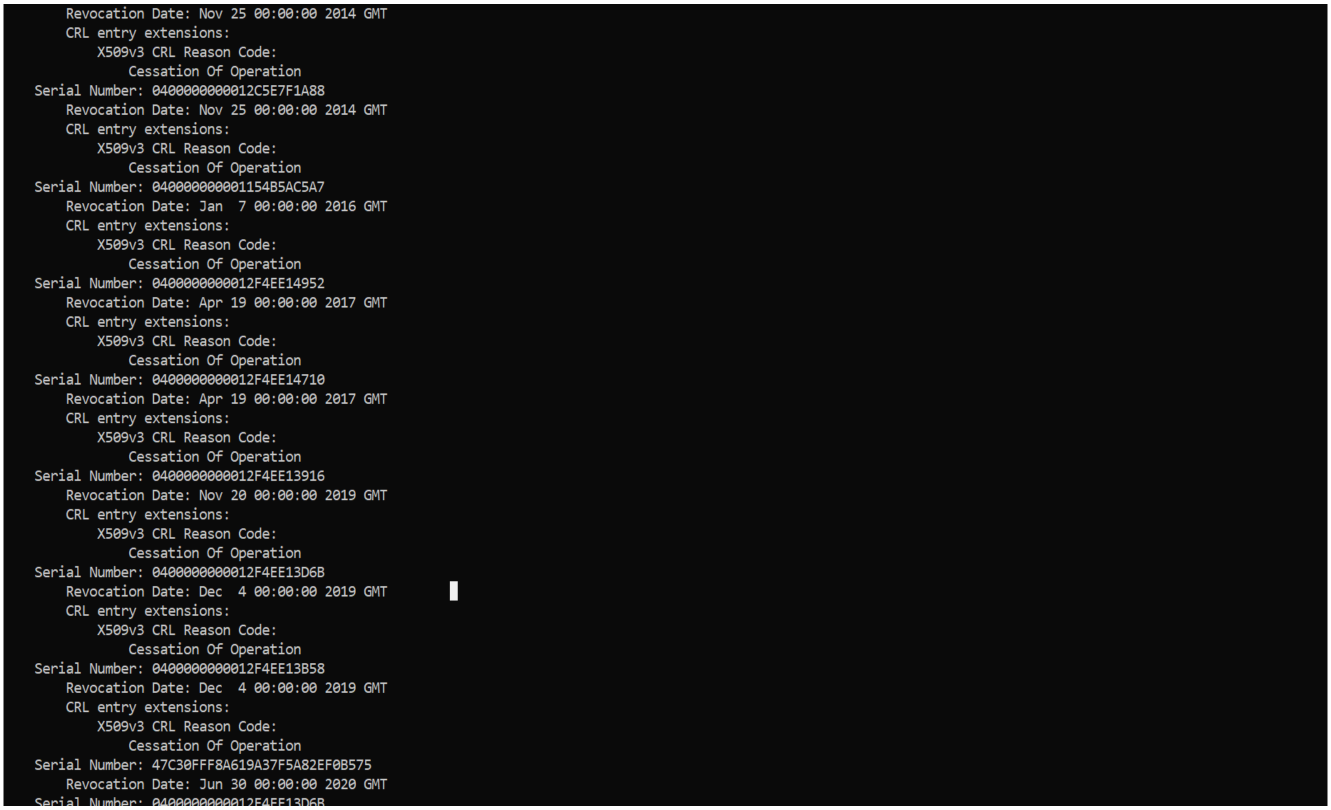
You can pick any two. Here are two valid ones from your list:

  - **Serial Number**: 0400000000011E44A5E404
  - **Revocation Date**: Nov 25 00:00:00 2014 GMT
  - **Serial Number**: 47C30FFF8A619A37F5A82EF0B575
  - **Revocation Date**: Jun 30 00:00:00 2020 GMT

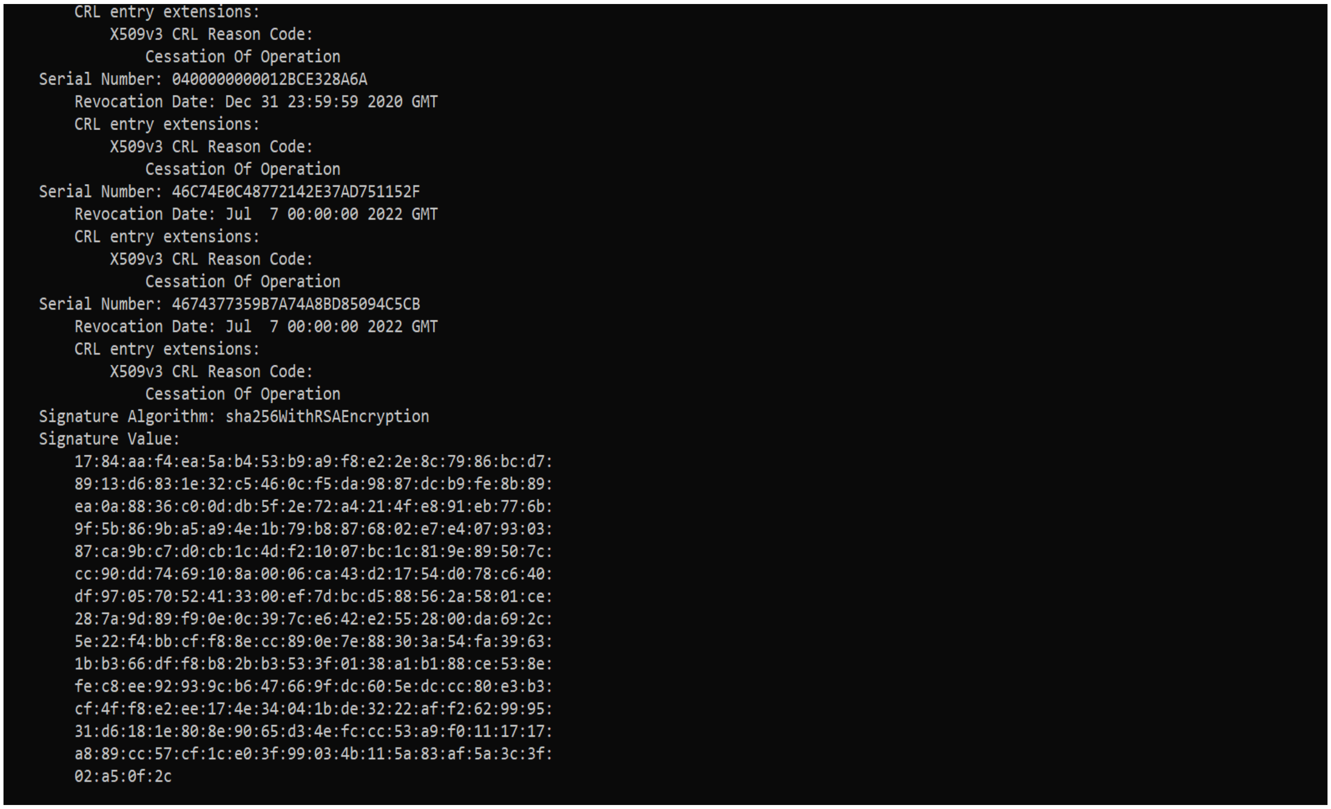
Emircan’s Screen



```
C:\Users\EMİRCAN>openssl crl -inform DER -in "C:\Users\EMİRCAN\OneDrive\Desktop\root.crl" -text -noout
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
        Last Update: Apr  7 00:00:00 2025 GMT
        Next Update: Jul 15 00:00:00 2025 GMT
        CRL extensions:
            X509v3 CRL Number:
                97
            X509v3 Authority Key Identifier:
                60:7B:66:1A:45:0D:97:CA:89:50:2F:7D:04:CD:34:A8:FF:FC:FD:4B
Revoked Certificates:
    Serial Number: 0400000000011E44A5E404
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012945C3A80F
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012019C18D68
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012C5E7F1A88
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000001154B5AC5A7
        Revocation Date: Jan  7 00:00:00 2016 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
```



```
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012C5E7F1A88
        Revocation Date: Nov 25 00:00:00 2014 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 040000000001154B5AC5A7
        Revocation Date: Jan  7 00:00:00 2016 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012F4EE14952
        Revocation Date: Apr 19 00:00:00 2017 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012F4EE14710
        Revocation Date: Apr 19 00:00:00 2017 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012F4EE13916
        Revocation Date: Nov 20 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012F4EE13D6B
        Revocation Date: Dec  4 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012F4EE13B58
        Revocation Date: Dec  4 00:00:00 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 47C30FFF8A619A37F5A82EF0B575
        Revocation Date: Jun 30 00:00:00 2020 GMT
    Serial Number: 0400000000012F4EE13D6B
```



```
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 0400000000012BCE328A6A
        Revocation Date: Dec 31 23:59:59 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 46C74E0C48772142E37AD751152F
        Revocation Date: Jul  7 00:00:00 2022 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Serial Number: 4674377359B7A74A8BD85094C5CB
        Revocation Date: Jul  7 00:00:00 2022 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Cessation Of Operation
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        17:84:aa:f4:ea:5a:b4:53:b9:a9:f8:e2:2e:8c:79:86:bc:d7:
        89:13:d6:83:1e:32:c5:46:0c:f5:da:98:87:dc:b9:fe:8b:89:
        ea:0a:88:36:c0:0d:db:5f:2e:72:a4:21:4f:e8:91:eb:77:6b:
        9f:5b:86:9b:a5:a9:4e:1b:79:b8:87:68:02:e7:e4:07:93:03:
        87:ca:9b:c7:d0:cb:1c:4d:f2:10:07:bc:1c:81:9e:89:50:7c:
        cc:90:dd:74:69:10:8a:00:06:ca:43:d2:17:54:d0:78:c6:40:
        df:97:05:70:52:41:33:00:ef:7d:bc:d5:88:56:2a:58:01:ce:
        28:7a:9d:89:f9:0e:0c:39:7c:e6:42:e2:55:28:00:da:69:2c:
        5e:22:f4:bb:cf:f8:8e:cc:89:0e:7e:88:30:3a:54:fa:39:63:
        1b:b3:66:df:f8:b8:2b:b3:53:3f:01:38:a1:b1:88:ce:53:8e:
        fe:c8:ee:92:93:9c:b6:47:66:9f:dc:60:5e:dc:cc:80:e3:b3:
        cf:4f:f8:e2:ee:17:4e:34:04:1b:de:32:22:af:f2:62:99:95:
        31:d6:18:1e:80:8e:90:65:d3:4e:fc:cc:53:a9:f0:11:17:17:
        a8:89:cc:57:cf:1c:e0:3f:99:03:4b:11:5a:83:af:5a:3c:3f:
        02:a5:0f:2c
```

Emircan’s Answers:

Two Revoked Certificates:

1. **Serial Number: `0400000000011E44A5E404`**
   Revocation Date: Nov 25, 2014
   Reason: Cessation Of Operation

2. **Serial Number: `040000000001154B5AC5A7`**
   Revocation Date: Jan 7, 2016
   Reason: Cessation Of Operation

Last Update's Date and Time:

- **Apr 7, 2025, 00:00:00 GMT**

Next Update's Date and Time:

- **Jul 15, 2025, 00:00:00 GMT**

Lessons Learned:

- **How to use `openssl crl` to read and analyze CRLs.**

- **Importance of specifying the correct file path using quotes if there are spaces or non-ASCII characters in the path.**

- **Structure and details found in a CRL: issuer, revoked serial numbers, revocation dates, reasons, etc.**

- **Practical understanding of certificate revocation in the Public Key Infrastructure (PKI) and why it’s important for maintaining trust.**

Q5-

Part A)

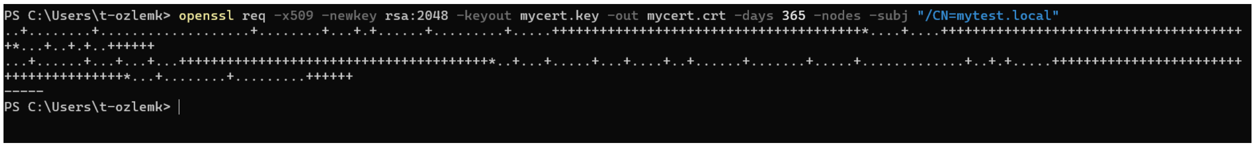
Command:

openssl req -x509 -newkey rsa:2048 -keyout mycert.key -out mycert.crt -days 365 -nodes -subj "/CN=mytest.local"

Explanation:

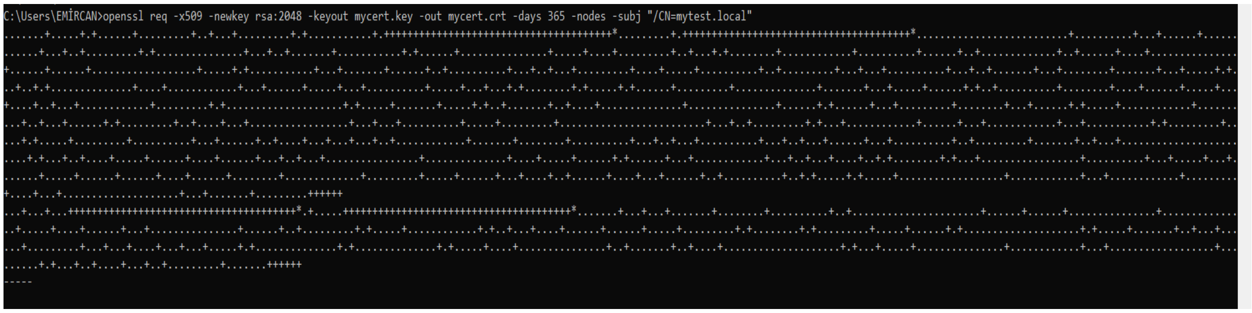
- `-x509`: Generate a self-signed certificate
- `-newkey rsa:2048`: Create a new 2048-bit RSA key pair
- `-keyout mycert.key`: Save private key to `mycert.key`
- `-out mycert.crt`: Save certificate to `mycert.crt`
- `-days 365`: Valid for 1 year
- `-nodes`: No password protection on private key (for easier use)
- `-subj "/CN=mytest.local"`: Common Name (hostname)

Özlem's Screen



```
PS C:\Users\t-ozlemk> openssl req -x509 -newkey rsa:2048 -keyout mycert.key -out mycert.crt -days 365 -nodes -subj "/CN=mytest.local"
..+........+...................+........+...+.+......+.........+.....+++++++++++++++++++++++++++++++++++++++++*....+....+++++++++++++++++++++++++++++++++++++++
+*...+..+.+..++++++
...+......+...+...+...++++++++++++++++++++++++++++++++++++++++*..+...+.....+...+....+..+......+.......+.....+.............+..+.+.....++++++++++++++++++++++++
+++++++++++++++*...+........+.........++++++
-----
PS C:\Users\t-ozlemk> |
```

Emircan's Screen



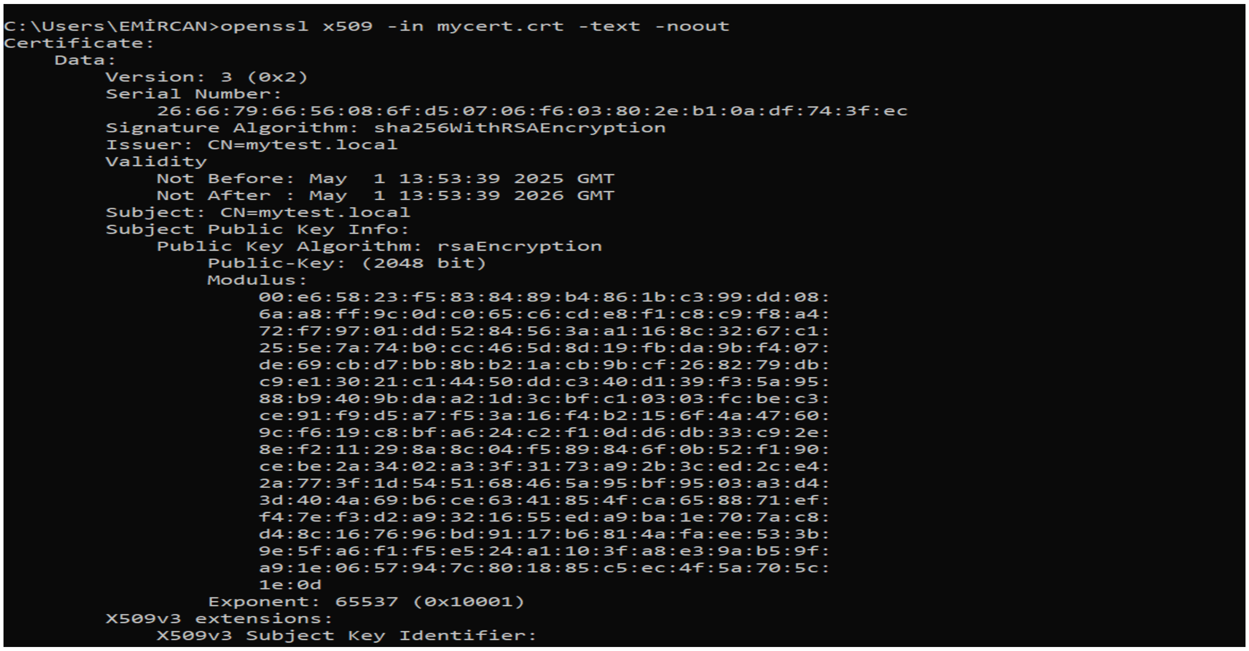
```
C:\Users\EMİRCAN>openssl req -x509 -newkey rsa:2048 -keyout mycert.key -out mycert.crt -days 365 -nodes -subj "/CN=mytest.local"
.......+.....+.+......+.........+..+...+...........+.........+.+...........+.+++++++++++++++++++++++++++++++++++++++++++++++++++*.........+.+++++++++++++++++++++++++++++++++++++++++++++++++++++*....................................+..........+...+......+......
......+...+..+.........+.+...............+...+........+...+..+.......+...........+.+.....+..........................+.....+....+.........+..+...+.+.........+.+........+............+..........+......+..+........+..+.............+..+......+....+...............
+......+......+..................+.....+.+.........+.+..........+...+.......+.....+..+.........+............+...+..+...+.........+....+.....+.........+...........+..+.........+...+...+..........+...+..+........+..+........+...+.........+.......+...+.....+.+.
..+..+.+.............+....+...........+...+........+...+......+.....+...+.........+....+...+...+.+.+...+...+.+........+.+.....+.+.....+.........+.........+.............+.......+...+.....+......+.+..+......+.+..+...........+.........+....+......+.....+...
+....+..+...+............+.........+.+..........+..................+.+.....+.......+.....+.+..+......+.+..+.......+..+....+..............+...............+......+.+......+...+.........+..+.........+...+......+.+.....+.............+.......
...+..+...+......+.+.........+..+....+...+.......+...+.................+...+...+..........+.....+.....+.....+.........+.........................+...+..+.....+...+..+.........+.+...+.............+......+...+.......+...+.............+...+............+.+..........+..
...+.+.....+.........+..........+...+......+..+.+......+..+....+...+...+...+..+...........+.......+...+........+.........+...........+...+..+...+.........+............+...+..+...+......+...+..........+..+........+..+.........+.......+..+...+..................
....+.+...+..+....+.....+......+....+......+..++......+..+..+...+................+..............+............+....+.....+......+.+......+...+.............+..............+...+..+...+....+..+.+........+.+...+.......+...+..................+...........+...+.....+...+.
.......+......+.......+.......+.....+.......+.........+..+.........+..............+.........+.....+......+...+.......+...+....+..+.......+....+...+......+..+...........+..........+..+.+.....+.+.....+...................+...........+.............+...+.............+........
+....+...+......................+...+........+............+.........++++++
...+...+...++++++++++++++++++++++++++++++++++++++++++++++++++*.+.....+++++++++++++++++++++++++++++++++++++++++++++++++++++*.......+...+...+.......+........+...+.........+..........+..+.........................+.....+.....+.......+.......+................+.............
..+.....+....+......+...+................+......+.....+......+..+.........+.+.....+...........+.+..+......+.+..+...+....+......+......+.....+.........+.+.........+.+........+.+..........+.....+......+.+..........+......................+.+.....+.......+..+...+...
...+.........+...+...+....+...+...+.....+.+..........+.+...............+.+...............+.+.....+....+.......+....+...............+..+.......+..+....+............+.....................+.+...+.....+................+............+.............+...+...................+...
......+.+...+..+....+...+..+.........+.......+.+.......++++++
-----
```

Part B)

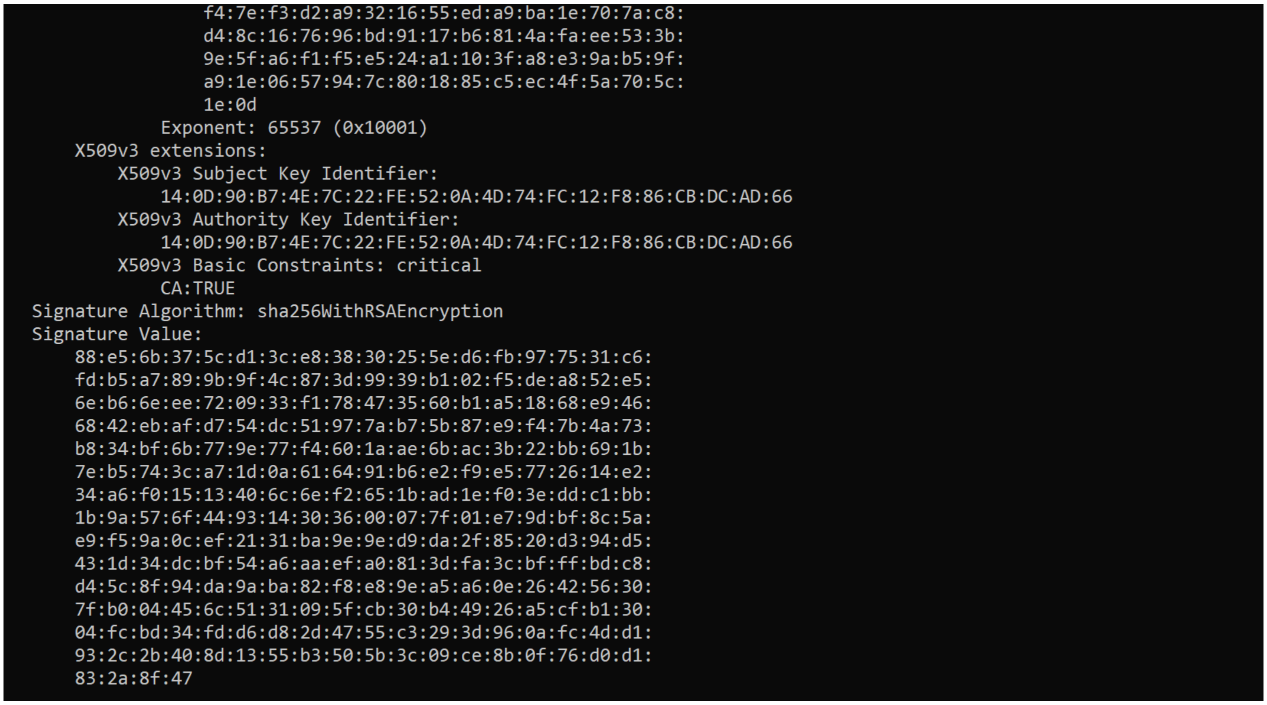
Command:

openssl x509 -in mycert.crt -text -noout

Emircan’s Screen

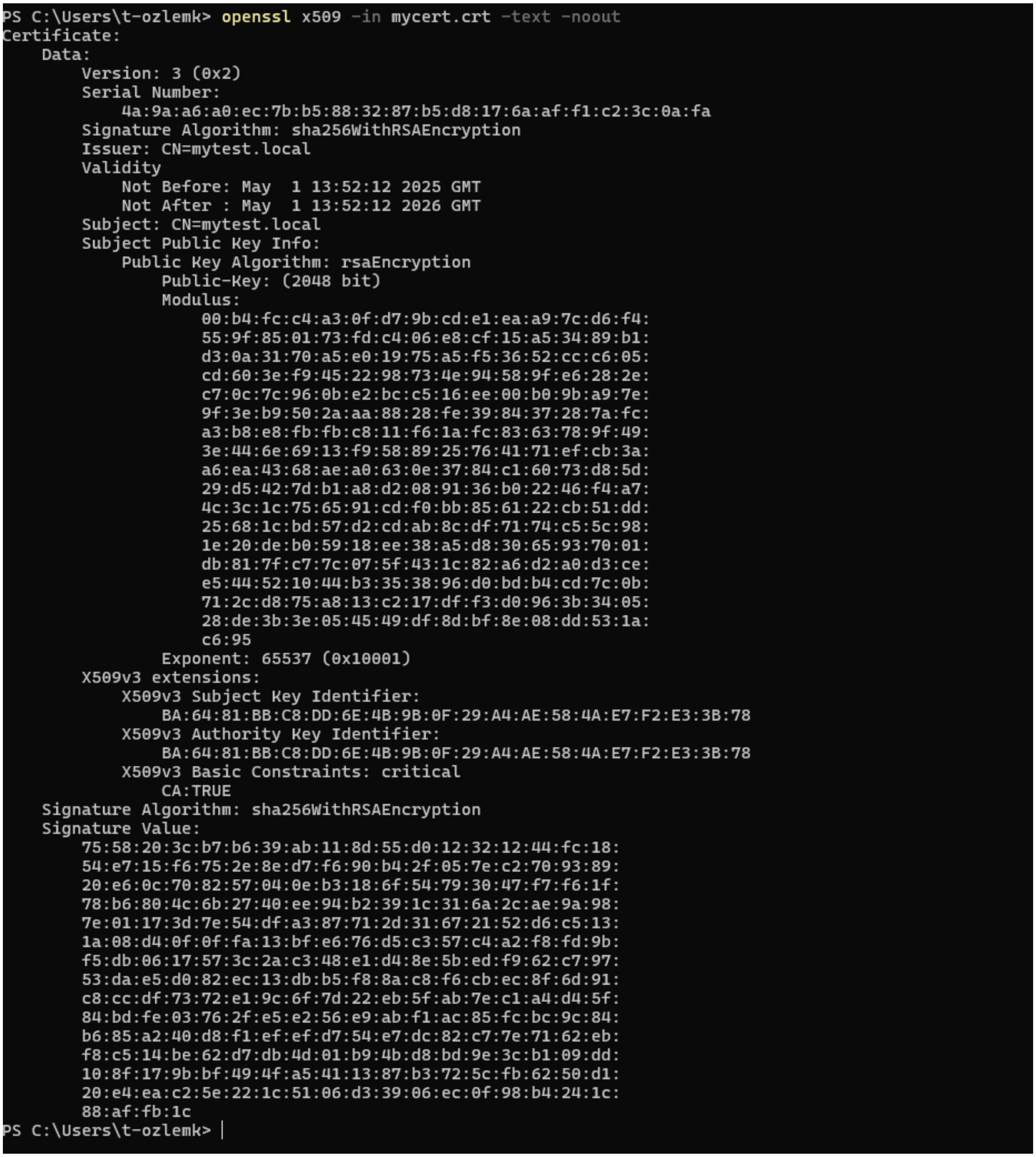


```
C:\Users\EMİRCAN>openssl x509 -in mycert.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:66:79:66:56:08:6f:d5:07:06:f6:03:80:2e:b1:0a:df:74:3f:ec
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=mytest.local
        Validity
            Not Before: May  1 13:53:39 2025 GMT
            Not After : May  1 13:53:39 2026 GMT
        Subject: CN=mytest.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e6:58:23:f5:83:84:89:b4:86:1b:c3:99:dd:08:
                    6a:a8:ff:9c:0d:c0:65:c6:cd:e8:f1:c8:c9:f8:a4:
                    72:f7:97:01:dd:52:84:56:3a:a1:16:8c:32:67:c1:
                    25:5e:7a:74:b0:cc:46:5d:8d:19:fb:da:9b:f4:07:
                    de:69:cb:d7:bb:8b:b2:1a:cb:9b:cf:26:82:79:db:
                    c9:e1:30:21:c1:44:50:dd:c3:40:d1:39:f3:5a:95:
                    88:b9:40:9b:da:a2:1d:3c:bf:c1:03:03:fc:be:c3:
                    ce:91:f9:d5:a7:f5:3a:16:f4:b2:15:6f:4a:47:60:
                    9c:f6:19:c8:bf:a6:24:c2:f1:0d:d6:db:33:c9:2e:
                    8e:f2:11:29:8a:8c:04:f5:89:84:6f:0b:52:f1:90:
                    ce:be:2a:34:02:a3:3f:31:73:a9:2b:3c:ed:2c:e4:
                    2a:77:3f:1d:54:51:68:46:5a:95:bf:95:03:a3:d4:
                    3d:40:4a:69:b6:ce:63:41:85:4f:ca:65:88:71:ef:
                    f4:7e:f3:d2:a9:32:16:55:ed:a9:ba:1e:70:7a:c8:
                    d4:8c:16:76:96:bd:91:17:b6:81:4a:fa:ee:53:3b:
                    9e:5f:a6:f1:f5:e5:24:a1:10:3f:a8:e3:9a:b5:9f:
                    a9:1e:06:57:94:7c:80:18:85:c5:ec:4f:5a:70:5c:
                    1e:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
```



```
                    f4:7e:f3:d2:a9:32:16:55:ed:a9:ba:1e:70:7a:c8:
                    d4:8c:16:76:96:bd:91:17:b6:81:4a:fa:ee:53:3b:
                    9e:5f:a6:f1:f5:e5:24:a1:10:3f:a8:e3:9a:b5:9f:
                    a9:1e:06:57:94:7c:80:18:85:c5:ec:4f:5a:70:5c:
                    1e:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                14:0D:90:B7:4E:7C:22:FE:52:0A:4D:74:FC:12:F8:86:CB:DC:AD:66
            X509v3 Authority Key Identifier:
                14:0D:90:B7:4E:7C:22:FE:52:0A:4D:74:FC:12:F8:86:CB:DC:AD:66
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        88:e5:6b:37:5c:d1:3c:e8:38:30:25:5e:d6:fb:97:75:31:c6:
        fd:b5:a7:89:9b:9f:4c:87:3d:99:39:b1:02:f5:de:a8:52:e5:
        6e:b6:6e:ee:72:09:33:f1:78:47:35:60:b1:a5:18:68:e9:46:
        68:42:eb:af:d7:54:dc:51:97:7a:b7:5b:87:e9:f4:7b:4a:73:
        b8:34:bf:6b:77:9e:77:f4:60:1a:ae:6b:ac:3b:22:bb:69:1b:
        7e:b5:74:3c:a7:1d:0a:61:64:91:b6:e2:f9:e5:77:26:14:e2:
        34:a6:f0:15:13:40:6c:6e:f2:65:1b:ad:1e:f0:3e:dd:c1:bb:
        1b:9a:57:6f:44:93:14:30:36:00:07:7f:01:e7:9d:bf:8c:5a:
        e9:f5:9a:0c:ef:21:31:ba:9e:9e:d9:da:2f:85:20:d3:94:d5:
        43:1d:34:dc:bf:54:a6:aa:ef:a0:81:3d:fa:3c:bf:ff:bd:c8:
        d4:5c:8f:94:da:9a:ba:82:f8:e8:9e:a5:a6:0e:26:42:56:30:
        7f:b0:04:45:6c:51:31:09:5f:cb:30:b4:49:26:a5:cf:b1:30:
        04:fc:bd:34:fd:d6:d8:2d:47:55:c3:29:3d:96:0a:fc:4d:d1:
        93:2c:2b:40:8d:13:55:b3:50:5b:3c:09:ce:8b:0f:76:d0:d1:
        83:2a:8f:47
```

Özlem’s Screen:



```
PS C:\Users\t-ozlemk> openssl x509 -in mycert.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4a:9a:a6:a0:ec:7b:b5:88:32:87:b5:d8:17:6a:af:f1:c2:3c:0a:fa
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=mytest.local
        Validity
            Not Before: May  1 13:52:12 2025 GMT
            Not After : May  1 13:52:12 2026 GMT
        Subject: CN=mytest.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b4:fc:c4:a3:0f:d7:9b:cd:e1:ea:a9:7c:d6:f4:
                    55:9f:85:01:73:fd:c4:06:e8:cf:15:a5:34:89:b1:
                    d3:0a:31:70:a5:e0:19:75:a5:f5:36:52:cc:c6:05:
                    cd:60:3e:f9:45:22:98:73:4e:94:58:9f:e6:28:2e:
                    c7:0c:7c:96:0b:e2:bc:c5:16:ee:00:b0:9b:a9:7e:
                    9f:3e:b9:50:2a:aa:88:28:fe:39:84:37:28:7a:fc:
                    a3:b8:e8:fb:fb:c8:11:f6:1a:fc:83:63:78:9f:49:
                    3e:44:6e:69:13:f9:58:89:25:76:41:71:ef:cb:3a:
                    a6:ea:43:68:ae:a0:63:0e:37:84:c1:60:73:d8:5d:
                    29:d5:42:7d:b1:a8:d2:08:91:36:b0:22:46:f4:a7:
                    4c:3c:1c:75:65:91:cd:f0:bb:85:61:22:cb:51:dd:
                    25:68:1c:bd:57:d2:cd:ab:8c:df:71:74:c5:5c:98:
                    1e:20:de:b0:59:18:ee:38:a5:d8:30:65:93:70:01:
                    db:81:7f:c7:7c:07:5f:43:1c:82:a6:d2:a0:d3:ce:
                    e5:44:52:10:44:b3:35:38:96:d0:bd:b4:cd:7c:0b:
                    71:2c:d8:75:a8:13:c2:17:df:f3:d0:96:3b:34:05:
                    28:de:3b:3e:05:45:49:df:8d:bf:8e:08:dd:53:1a:
                    c6:95
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                BA:64:81:BB:C8:DD:6E:4B:9B:0F:29:A4:AE:58:4A:E7:F2:E3:3B:78
            X509v3 Authority Key Identifier:
                BA:64:81:BB:C8:DD:6E:4B:9B:0F:29:A4:AE:58:4A:E7:F2:E3:3B:78
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        75:58:20:3c:b7:b6:39:ab:11:8d:55:d0:12:32:12:44:fc:18:
        54:e7:15:f6:75:2e:8e:d7:f6:90:b4:2f:05:7e:c2:70:93:89:
        20:e6:0c:70:82:57:04:0e:b3:18:6f:54:79:30:47:f7:f6:1f:
        78:b6:80:4c:6b:27:40:ee:94:b2:39:1c:31:6a:2c:ae:9a:98:
        7e:01:17:3d:7e:54:df:a3:87:71:2d:31:67:21:52:d6:c5:13:
        1a:08:d4:0f:0f:fa:13:bf:e6:76:d5:c3:57:c4:a2:f8:fd:9b:
        f5:db:06:17:57:3c:2a:c3:48:e1:d4:8e:5b:ed:f9:62:c7:97:
        53:da:e5:d0:82:ec:13:db:b5:f8:8a:c8:f6:cb:ec:8f:6d:91:
        c8:cc:df:73:72:e1:9c:6f:7d:22:eb:5f:ab:7e:c1:a4:d4:5f:
        84:bd:fe:03:76:2f:e5:e2:56:e9:ab:f1:ac:85:fc:bc:9c:84:
        b6:85:a2:40:d8:f1:ef:ef:d7:54:e7:dc:82:c7:7e:71:62:eb:
        f8:c5:14:be:62:d7:db:4d:01:b9:4b:d8:bd:9e:3c:b1:09:dd:
        10:8f:17:9b:bf:49:4f:a5:41:13:87:b3:72:5c:fb:62:50:d1:
        20:e4:ea:c2:5e:22:1c:51:06:d3:39:06:ec:0f:98:b4:24:1c:
        88:af:fb:1c
PS C:\Users\t-ozlemk>
```

What these screens shows:

- Certificate version
- Serial number

- Signature algorithm
- Issuer and Subject (should match)
- Validity (Not Before / Not After)
- Public key details