

# Confidential Computing – Assignment 1

Submit by: Noam Tarshish (207761024) & Daniel Hodisan (205795016) & Lavi Ben-Shimol (3307866756)

## Creating Digital Certificates

1. Firstly, we generate the RSA private key for the root CSA using this command:

```
openssl genrsa -out rootCA.key 3072
```

then, we create the self-signed root certificate with serial number 01 using this command:

```
openssl req -x509 -new -nodes -key rootCA.key -sha384 -days 1095 -out rootCA.crt -set_serial 01
```

Those are the details of the generated root certificate:

```
-----(kali@kali)-[~]
+ openssl x509 -text -noout -in rootCA.crt
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=IL, ST=Israel, L=Beer Sheva, O=BGU, OU=BGU
    Validity
      Not Before: Apr 7 14:31:06 2025 GMT
      Not After : Apr 6 14:31:06 2028 GMT
    Subject: C=IL, ST=Israel, L=Beer Sheva, O=BGU, OU=BGU
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (3072 bit)
      Modulus:
        00:f9:ba:35:a4:95:0a:4d:27:93:0f:f3:86:93:49:
        42:92:7a:cd:9d:6b:b9:d9:00:5a:19:3a:a6:a4:76:f
        59:f6:a1:db:05:b4:71:0f:c1:8a:71:0a:c3:53:a4:
        3b:c6:b2:22:f8:b7:24:43:ab:15:03:c4:62:c7:95:f
        3e:a0:86:00:0a:9e:02:a9:0b:ab:9d:0b:0d:24:5a:
        b0:9a:1f:da:63:b2:c0:21:ac:9d:2b:d5:12:91:1b:
        8e:d6:e5:93:db:f0:56:63:cf:20:c7:00:7d:95:18:
        37:c7:09:1e:37:e4:cd:30:03:63:fc:a1:3e:0a:35:
        ac:e8:86:e8:97:dd:bb:ec:15:1f:5d:a1:00:15:f1:
        2e:03:ac:1d:72:e6:19:6c:c3:ac:0c:21:9a:df:30:
        37:fb:fa:a9:ed:30:65:5a:16:05:0d:a1:0a:ee:40:
        32:d7:5a:5b:09:4a:12:5e:f9:48:ed:6d:f0:6c:7d:
        0e:c7:2b:74:6c:97:11:d1:22:78:0b:02:c0:00:18:
        55:05:54:12:d7:a2:7b:9d:de:c1:ca:96:0c:73:69:
        c0:42:0a:81:a2:06:48:7a:cb:ea:91:a9:3c:17:4a:
        2e:30:f2:1e:30:1c:80:1a:8a:87:7d:aa:cf:ae:df:
        45:cf:6a:d4:69:4a:ab:0f:4a:fd:0b:b6:b6:44:33:
        00:8a:0c:37:01:2d:8e:56:2b:9f:23:aa:f6:ae:8d:
        c0:5f:e1:75:60:9f:cb:aa:de:20:0a:b4:20:2a:b2:
        ea:82:06:f1:ea:f2:1f:aa:74:32:16:97:96:a0:ae:
        f2:11:af:f6:55:ac:1e:f6:76:9a:4a:5a:07:56:
        31:e5:13:7c:ba:09:ca:11:db:30:00:cd:ac:51:f2:
        32:0d:02:0f:0a:eb:03:90:ca:40:c0:29:0f:72:ed:
        b0:36:09:c1:0d:a1:07:ed:09:ea:c1:59:03:e2:17:
        d9:b2:ae:ee:d1:b9:65:19:f1:b0:6b:42:76:2c:38:
        91:0e:1a:c5:2b:72:78:91:dc:73
      Exponent: 65537 (0x10001)
```

```
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    1D:31:FD:A7:9C:45:46:87:82:28:EA:4B:DD:15:7E:4E:2F:5C:1C:2F
  X509v3 Authority Key Identifier:
    1D:31:FD:A7:9C:45:46:87:82:28:EA:4B:DD:15:7E:4E:2F:5C:1C:2F
  X509v3 Basic Constraints: critical
    CA:TRUE
  Signature Algorithm: sha384WithRSAEncryption
  Signature Value:
    aa:e7:e0:4c:50:4f:49:8a:f1:fb:c4:9e:aa:02:05:fb:b4:7d:
    fa:9d:ed:81:3a:9a:b1:4a:8d:13:fb:35:fe:24:57:1c:ec:42:
    f0:6b:69:6c:ed:26:e5:d7:75:46:ec:34:27:bd:71:f2:c3:02:
    fb:69:3c:5d:0b:f7:a6:b4:1c:1e:fe:ad:3a:42:04:a8:f2:69:
    ac:69:9f:6a:03:53:f1:e8:04:02:dc:f2:5f:9f:07:72:e5:96:
    97:70:f5:4a:43:ee:c8:61:07:3c:22:03:64:f6:5c:7b:de:b5:
    1e:b9:9f:6f:0d:5c:d5:74:45:92:ee:3b:75:09:6a:fd:f6:07:
    37:22:d8:22:15:05:ed:0e:a1:4f:3d:b0:5c:de:6e:28:a3:d8:
    74:92:a8:9a:ec:18:cf:7b:ee:d4:00:14:50:f0:4a:f3:cf:60:
    31:e1:38:9e:5a:d0:70:78:4f:f9:fd:97:00:1a:27:0b:d5:36:
    f8:ee:b1:29:59:a2:ce:58:42:f0:3f:37:3f:21:f9:11:65:f9:
    79:75:cd:10:76:04:26:d0:c3:23:48:f0:32:06:42:77:7c:53:
    39:df:ed:2a:cc:a0:06:74:97:51:ac:23:0e:a3:23:00:68:a8:
    7d:91:a7:27:5b:fb:2f:5b:b9:02:61:62:ce:03:a8:5f:ee:ca:
    c2:ea:af:0d:97:a0:08:da:9e:ef:57:09:c6:9e:90:4d:a3:07:
    70:54:4c:03:7a:7f:9c:07:0c:6a:95:cd:26:1c:f5:e9:9c:ea:
    d7:20:91:7c:6b:77:2c:26:38:df:16:14:8c:72:5a:b2:b2:ed:
    bb:ca:3c:4d:f9:cd:b1:39:4c:ef:c0:0a:53:fc:37:26:a3:68:
    cb:d2:a4:8c:d0:cf:ef:31:75:45:dc:ee:ab:08:0d:06:60:55:
    ac:cb:bb:70:e0:63:ed:aa:c8:7a:d5:0d:49:23:56:94:eb:eb:
    55:1d:ed:52:1d:70:79:84:49:74:b9:c1:f2:47:79:31:1d:ef:
    59:1d:99:77:34:0b
```

2. we generate Alice's RSA key pair and certificate for Alice with those steps:

Generate Alice's RSA private key:

```
openssl genrsa -out alice.key 3072
```

Create Alice's Certificate Signing Request (CSR) :

```
openssl req -new -key alice.key -out alice.csr -sha384
```

Sign Alice's CSR with the root CA:

```
openssl x509 -req -in alice.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out alice.crt -days 365 -sha384 -set_serial 02
```

We got the certificate:

```
-----(kali@kali)-[~]
+ openssl x509 -text -noout -in alice.crt
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=IL, ST=Israel, L=Beer Sheva, O=BGU, OU=BGU
    Validity
      Not Before: Apr 7 14:41:58 2025 GMT
      Not After : Apr 7 14:41:58 2026 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=Alice
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (3072 bit)
      Modulus:
        00:e5:10:6b:64:bf:11:2f:8a:89:f9:12:aa:bf:8c:
        e4:4d:01:26:1c:68:5e:3c:b9:7b:da:b1:e6:d0:4a:
        aa:cb:9c:43:9e:f4:6b:58:3d:b8:c2:6a:03:ec:ab:
        b6:a3:76:00:eb:7b:64:a6:7c:89:d9:7a:3c:3d:a5:
        dc:f7:d5:a8:60:93:a2:f5:f1:36:0a:0d:fd:99:5e:
        dk:02:22:da:ab:fc:3c:86:64:9e:32:6b:80:ad:72:
        35:4e:49:ba:9f:8d:7f:c3:10:c7:35:7f:bd:e3:59:
        5d:36:9d:e6:63:cb:76:61:80:ac:0a:3b:34:2e:a6:
        e3:ca:9d:35:51:f0:ca:a7:56:1f:06:23:84:67:10:
        e9:50:20:01:60:57:51:0d:01:fe:b5:5c:0e:67:70:
        ee:0d:81:46:34:22:7b:50:85:d8:da:c5:ee:1d:3f:
        14:b8:4d:f4:d8:26:0f:80:12:af:29:b4:ac:5a:eb:
        cb:70:a6:7b:33:b2:49:ba:d3:cc:7e:99:66:1f:a7:
        07:71:37:53:d7:05:e3:55:49:65:65:6e:3c:04:cb:
        46:ae:c1:07:d2:62:77:1e:2e:1e:09:b5:4b:40:d4:
        58:fa:59:a2:2d:44:59:9c:ec:54:86:8e:c3:1b:b6:
        b4:4f:92:08:3f:e5:93:76:fd:0d:f5:5a:c6:72:ef:
        6a:35:24:13:8d:07:fa:18:e7:b2:5d:8c:f3:d0:42:
        94:4d:5e:a3:6e:f1:ca:ee:ba:bc:19:3d:a0:58:e3:
        12:92:c4:36:6f:9a:10:2e:19:09:01:fe:b5:5c:0e:67:70:
        38:5f:2e:a3:ca:0a:45:ce:6e:fd:94:5d:8c:b2:bc:9d:
        99:31:51:d6:96:58:8a:16:c5:b8:3e:ff:1c:0b:21:
        5d:1d:a3:dd:88:57:71:12:f5:6b:8b:8d:43:24:bf:
        e7:b7:b6:cd:cb:a7:d6:80:51:d7:22:c5:09:e6:ae:
        f3:ec:bc:35:5f:98:41:39:1e:0e:ee:52:ab:da:d7:
        56:d0:88:00:8e:b5:41:57:c8:13
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      83:DB:FF:35:BD:45:C5:14:78:FC:7E:AA:38:83:3A:E3:8E:DA:C3:39
    X509v3 Authority Key Identifier:
      1D:31:FD:A7:9C:45:46:87:82:28:EA:4B:DD:15:7E:4E:2F:5C:1C:2F
    Signature Algorithm: sha384WithRSAEncryption
    Signature Value:
      60:23:d5:2d:7c:33:d2:19:8c:9e:7a:a1:10:c1:7d:dc:47:d3:
      2f:32:78:6c:6e:fe:95:64:6e:71:7c:ef:a6:a6:b6:e4:93:62:
      1e:12:91:6d:76:87:31:50:12:39:d2:1f:62:1d:f0:78:3a:3d:
      0b:de:16:b8:8c:35:da:05:b9:3a:20:31:90:66:eb:58:58:4d:
      1a:8b:a4:cf:29:05:97:35:78:6a:81:e0:f5:80:c6:3c:de:23:
      d8:b2:6d:b1:3c:0e:86:fd:2a:c4:ff:d6:7b:be:ec:b0:54:88:
      0d:7e:03:e1:4c:6a:d9:bf:30:85:fc:10:04:38:3c:78:29:dd:
      22:be:f1:52:14:98:a9:32:cd:04:01:fe:3a:e0:56:63:3d:66:
      1d:f0:b7:05:87:d7:c6:44:ac:42:59:06:31:b4:d8:cb:d4:9f:
      fe:81:df:cb:bb:8f:44:b1:44:44:31:96:e4:e0:ad:7a:08:e5:77:
      fa:d7:10:f2:08:14:0f:34:3c:0d:c5:10:dc:6c:18:83:19:5d:
      77:29:4b:7b:8d:05:04:23:b5:21:53:fe:93:3d:d6:e1:b3:d5:
      40:4f:69:47:c9:3f:17:2b:c3:02:b1:d0:aa:5c:34:07:a2:c4:
      29:2d:c3:e0:e4:09:2f:19:aa:19:e0:d1:d1:34:46:bb:8a:1d:
      49:99:66:f0:07:d0:56:ad:d2:99:e7:24:1e:09:7f:63:40:54:
      03:74:9f:c7:b1:8e:ee:8d:43:7d:50:91:bd:69:1a:93:c2:dc:
      be:85:33:73:ef:07:3e:8b:4d:c7:4a:12:bf:3d:e2:01:c5:e7:
      ce:03:1a:5d:30:0f:09:46:2a:8e:db:e9:be:ee:bb:28:1f:a9:
      5a:22:33:34:4f:a4:07:b3:7d:be:fb:c8:ba:7f:75:47:33:fc:
      5f:d9:24:c4:bf:a3:e7:d3:ec:67:90:0c:a3:58:a8:3b:ac:9a:
      c8:4b:19:c2:57:b9:1e:9c:3e:b6:91:4a:07:35:2f:a5:5f:ed:
      17:00:95:d7:73:91
```

3. we generate Bob's RSA key pair and certificate for Alice with those steps:

Generate Bob's RSA private key:

```
openssl genrsa -out bob.key 3072
```

Create Alice's Certificate Signing Request (CSR):

```
openssl req -new -key bob.key -out bob.csr -sha384
```

Sign Bob's CSR with the root CA:

```
openssl x509 -req -in bob.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out alice.crt -days 365 -sha384 -set_serial 03
```

We got the certificate:

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 3 (0x3)
  Signature Algorithm: sha384WithRSAEncryption
  Issuer: C=IL, ST=Israel, L=Beer Sheva, O=BGU, OU=BGU
  Validity
    Not Before: Apr  7 14:49:14 2025 GMT
    Not After : Apr  7 14:49:14 2026 GMT
  Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=Bob
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (3072 bit)
    Modulus:
      00:c5:99:39:31:29:f6:1c:50:3d:f4:2f:2e:c9:d7:
      32:ef:8a:25:a9:8a:5b:ce:ae:07:6d:bf:55:88:a7:
      48:95:a5:38:f9:d4:58:3c:38:f0:81:f5:9d:9b:ff:
      7a:ed:33:6f:3c:23:ff:f3:ad:2c:94:8b:ee:a4:7d:
      a1:80:f5:f8:b9:e5:4a:9f:63:8f:47:c0:9c:38:b9:
      82:86:29:b9:76:1d:26:77:b0:6d:d3:19:22:4e:1a:
      89:53:bb:50:0d:43:5c:0e:3f:e4:d1:5e:68:49:52:
      60:d1:2e:ca:43:31:95:40:34:23:73:a3:65:94:a2:
      af:29:98:9b:0d:74:49:8d:3d:7b:ae:5e:b6:9a:a6:
      e9:72:e0:b2:75:8e:6f:b8:58:97:9a:1d:13:df:3a:
      ed:eb:88:0f:c5:b2:44:1e:27:7a:6c:4c:03:4c:75:
      c8:ae:d0:39:1e:30:db:7b:aa:95:1d:27:c8:b4:ee:
      c5:16:9d:fb:0d:52:ec:ec:1b:c2:ba:d3:61:cd:74:
      b1:12:16:e9:36:df:bb:f2:3c:8c:e7:1b:49:81:dd:
      df:16:09:0b:ac:b3:53:af:27:85:e2:4e:e3:d2:de:
      39:56:fb:f9:20:7d:29:ea:41:26:e4:6c:7f:43:22:
      65:bd:dc:8f:67:6d:08:74:56:0f:01:68:06:e5:33:
      fc:35:4e:8c:90:ee:fb:c2:82:db:34:cb:b2:0f:18:
      de:b6:90:95:64:ae:b2:3d:b9:93:ae:dd:a4:60:a8:
      3f:2b:be:50:6b:24:1e:e5:ed:ab:16:e8:af:d1:e3:
      de:76:04:32:ff:35:1f:66:02:08:f3:8f:05:fe:0f:
      7b:48:94:99:b6:b3:3d:b7:5c:a6:55:a7:b1:93:b7:
      82:ab:b4:4b:50:8e:e1:47:d5:dd:e0:cb:c4:13:19:
      ab:8e:07:e3:bf:35:86:ea:21:c1:14:e1:31:9a:cb:
      32:84:c5:cb:7b:bf:df:c6:62:ed:80:75:4f:7a:8b:
      34:72:b7:e2:09:ed:b5:a1:f9:55
    Exponent: 65537 (0x10001)

X509v3 extensions:
  X509v3 Subject Key Identifier:
    2E:C1:B5:10:3F:E2:BD:10:36:22:CD:34:8B:25:09:EB:02:E3:DE:62
  X509v3 Authority Key Identifier:
    1D:31:FD:A7:9C:45:46:87:B2:28:EA:4B:DD:15:7E:4E:2F:5C:C2:CF
  Signature Algorithm: sha384WithRSAEncryption
  Signature Value:
    57:9e:ca:21:ab:93:ad:8f:95:99:f3:ac:77:75:7c:c1:80:45:
    7d:44:3c:22:d5:3f:30:03:85:85:18:b2:47:1d:9c:d6:b6:90:
    cc:0e:2b:61:0c:d3:ba:21:aa:25:0f:85:c4:ca:78:d3:75:39:
    7d:e4:5b:b5:d3:47:9c:90:4b:51:68:a1:7c:8e:d5:1c:6e:25:
    69:61:53:8c:68:31:36:97:e2:e1:e3:e0:48:72:53:4f:ba:c6:
    62:72:c9:b2:4d:2b:42:2d:16:39:fd:ea:ce:37:99:eb:34:0d:
    ba:4a:a0:4d:9e:3b:67:0e:5a:57:37:10:04:d6:66:9c:10:cc:
    d7:93:14:44:19:0a:98:7a:90:b0:07:64:17:e9:4a:44:fe:e1:
    a2:99:4f:80:56:11:7b:3f:b2:74:43:db:6c:d6:28:1b:fc:56:
    50:37:9a:a1:7b:02:80:c8:94:85:fa:98:40:9d:9a:1b:77:40:
    fe:93:09:01:d2:0f:7c:4f:00:37:37:79:98:f3:20:8f:f1:23:
    e3:b9:c8:77:99:cb:a8:34:6f:50:8b:33:26:26:f1:30:79:df:
    dd:84:f2:0b:48:ed:1b:fb:9b:73:54:78:9c:4a:cb:5e:aa:2d:
    a4:71:94:02:2b:dd:8a:14:98:5f:92:d2:2b:b6:a7:57:76:ea:
    35:bb:42:9f:19:02:51:1a:4f:24:28:c7:04:k1:da:d2:29:6e:
    f0:fc:76:30:97:90:55:13:18:10:04:c1:7f:37:4c:de:0b:97:
    91:20:2e:0f:cf:f8:11:d2:ae:00:e8:8e:d0:8c:32:07:6a:c3:
    06:46:98:a5:9c:69:88:3b:5d:dd:39:f3:28:87:8e:29:d1:b1:
    02:8b:bd:d8:c3:e9:f6:63:5d:0b:3c:e4:4b:28:27:73:05:7b:
    6a:73:15:02:c6:a0:8f:2f:da:a0:6e:a4:46:b7:99:d0:09:d5:
    78:2f:d7:f2:94:13:cc:25:15:a8:c8:6b:6e:ea:5b:8d:15:c6:
    10:d2:00:40:a2:e5
```

