Secure Boot Template

Q1. Extract the Microsoft certificate that belongs to the key referred to in Step 1 from the UEFI firmware and show its text representation on your log Hint mokutil openssl x509

The command “mokutil –export” produced the output:

- MOK-0001.der
- MOK-0002.der

The command “mokutil –export –db” produced the output:

- DB-0001.der
- DB-0002.der

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:08:d3:c4:00:00:00:00:00:04
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Washington, L = Redmond, O = Microsoft
Corporation, CN = Microsoft Corporation Third Party Marketplace Root
        Validity
            Not Before: Jun 27 21:22:45 2011 GMT
            Not After : Jun 27 21:32:45 2026 GMT
        Subject: C = US, ST = Washington, L = Redmond, O = Microsoft
Corporation, CN = Microsoft Corporation UEFI CA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a5:08:6c:4c:c7:45:09:6a:4b:0c:a4:c0:87:7f:
                    06:75:0c:43:01:54:64:e0:16:7f:07:ed:92:7d:0b:
                    b2:73:bf:0c:0a:c6:4a:45:61:a0:c5:16:2d:96:d3:
                    f5:2b:a0:fb:4d:49:9b:41:80:90:3c:b9:54:fd:e6:
                    bc:d1:9d:c4:a4:18:8a:7f:41:8a:5c:59:83:68:32:
                    bb:8c:47:c9:ee:71:bc:21:4f:9a:8a:7c:ff:44:3f:
                    8d:8f:32:b2:26:48:ae:75:b5:ee:c9:4c:1e:4a:19:
                    7e:e4:82:9a:1d:78:77:4d:0c:b0:bd:f6:0f:d3:16:
                    d3:bc:fa:2b:a5:51:38:5d:f5:fb:ba:db:78:02:db:
                    ff:ec:0a:1b:96:d5:83:b8:19:13:e9:b6:c0:7b:40:
                    7b:e1:1f:28:27:c9:fa:ef:56:5e:1c:e6:7e:94:7e:
                    c0:f0:44:b2:79:39:e5:da:b2:62:8b:4d:bf:38:70:
                    e2:68:24:14:c9:33:a4:08:37:d5:58:69:5e:d3:7c:
                    ed:c1:04:53:08:e7:4e:b0:2a:87:63:08:61:6f:63:
                    15:59:ea:b2:2b:79:d7:0c:61:67:8a:5b:fd:5e:ad:
                    87:7f:ba:86:67:4f:71:58:12:22:04:22:22:ce:8b:
                    ef:54:71:00:ce:50:35:58:76:95:08:ee:6a:b1:a2:
```

```
                    01:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.21.1:
                .....
            1.3.6.1.4.1.311.21.2:
                ....k..wSJ.%7.N.&{. p.
            X509v3 Subject Key Identifier:
                13:AD:BF:43:09:BD:82:70:9C:8C:D5:4F:31:6E:D5:22:98:8A:1B:D4
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:
                45:66:52:43:E1:7E:58:11:BF:D6:4E:9E:23:55:08:3B:3A:22:6A:A8
            X509v3 CRL Distribution Points:
                Full Name:
URI:http://crl.microsoft.com/pki/crl/products/MicCorThiParMarRoo_2010-10-05.
crl
            Authority Information Access:
                CA Issuers -
URI:http://www.microsoft.com/pki/certs/MicCorThiParMarRoo_2010-10-05.crt
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        35:08:42:ff:30:cc:ce:f7:76:0c:ad:10:68:58:35:29:46:32:
        76:27:7c:ef:12:41:27:42:1b:4a:aa:6d:81:38:48:59:13:55:
        f3:e9:58:34:a6:16:0b:82:aa:5d:ad:82:da:80:83:41:06:8f:
        b4:1d:f2:03:b9:f3:1a:5d:1b:f1:50:90:f9:b3:55:84:42:28:
        1c:20:bd:b2:ae:51:14:c5:c0:ac:97:95:21:1c:90:db:0f:fc:
        77:9e:95:73:91:88:ca:bd:bd:52:b9:05:50:0d:df:57:9e:a0:
        61:ed:0d:e5:6d:25:d9:40:0f:17:40:c8:ce:a3:4a:c2:4d:af:
        9a:12:1d:08:54:8f:bd:c7:bc:b9:2b:3d:49:2b:1f:32:fc:6a:
        21:69:4f:9b:c8:7e:42:34:fc:36:06:17:8b:8f:20:40:c0:b3:
        9a:25:75:27:cd:c9:03:a3:f6:5d:d1:e7:36:54:7a:b9:50:b5:
        d3:12:d1:07:bf:bb:74:df:dc:1e:8f:80:d5:ed:18:f4:2f:14:
        16:6b:2f:de:66:8c:b0:23:e5:c7:84:d8:ed:ea:c1:33:82:ad:
        56:4b:18:2d:f1:68:95:07:cd:cf:f0:72:f0:ae:bb:dd:86:85:
        98:2c:21:4c:33:2b:f0:0f:4a:f0:68:87:b5:92:55:32:75:a1:
        6a:82:6a:3c:a3:25:11:a4:ed:ad:d7:04:ae:cb:d8:40:59:a0:
        84:d1:95:4c:62:91:22:1a:74:1d:8c:3d:47:0e:44:a6:e4:b0:
        9b:34:35:b1:fa:b6:53:a8:2c:81:ec:a4:05:71:c8:9d:b8:ba:
        e8:1b:44:66:e4:47:54:0e:8e:56:7f:b3:9f:16:98:b2:86:d0:
        68:3e:90:23:b5:2f:5e:8f:50:85:8d:c6:8d:82:5f:41:a1:f4:
        2e:0d:e0:99:d2:6c:75:e4:b6:69:b5:21:86:fa:07:d1:f6:e2:
        4d:d1:da:ad:2c:77:53:1e:25:32:37:c7:6c:52:72:95:86:b0:
        f1:35:61:6a:19:f5:b2:3b:81:50:56:a6:32:2d:fe:a2:89:f9:
```

```
        42:86:27:18:55:a1:82:ca:5a:9b:f8:30:98:54:14:a6:47:96:
        25:2f:c8:26:e4:41:94:1a:5c:02:3f:e5:96:e3:85:5b:3c:3e:
        3f:bb:47:16:72:55:e2:25:22:b1:d9:7b:e7:03:06:2a:a3:f7:
        1e:90:46:c3:00:0d:d6:19:89:e3:0e:35:27:62:03:71:15:a6:
        ef:d0:27:a0:a0:59:37:60:f8:38:94:b8:e0:78:70:f8:ba:4c:
        86:87:94:f6:e0:ae:02:45:ee:65:c2:b6:a3:7e:69:16:75:07:
        92:9b:f5:a6:bc:59:83:58
```

Q2. Is this certificate the root certificate in the chain of trust? Is it the ultimate root of trust? What is the role of the Platform Key (PK)?

Yes, it is the root certificate in the chain of trust, but it is not the ultimate root of trust. The ultimate root of trust is the Platform Key (PK). Only updates signed by the PK can modify the Key Exchange Key (KEK) database, which in turn manages updates to the signature database (DB) and the forbidden signature database (DBX). The PK's role is to ensure that any changes to the KEK are properly authorized, thereby maintaining the integrity of the boot process. Since the PK is typically owned and managed by the platform manufacturer, it establishes a reliable and secure foundation for the system.

Q3. Verify that the system indeed boots the shim boot loader in the first stage What is the full path name of this boot loader?

```
sudo efibootmgr -v
BootCurrent: 0003
Timeout: 0 seconds
BootOrder: 0003,0000,0001,0002
Boot0000* ubuntu
HD(1,GPT,8d3dcf8c-8350-49fc-85eb-9315bc22579e,0x800,0x219800)/File(\EFI\ubun
tu\shimx64.efi)
Boot0001* Onboard NIC(IPV4)
PciRoot(0x0)/Pci(0x19,0x0)/MAC(b8ca3a92d9bf,0)/IPv4(0.0.0.00.0.0.0,0,0)AMBO
Boot0002* Onboard NIC(IPV6)
PciRoot(0x0)/Pci(0x19,0x0)/MAC(b8ca3a92d9bf,0)/IPv6([::]:<->[::]:,0,0)AMBO
Boot0003* debian    HD(1,GPT,6c2720cf-9e7d-41d6-
be26-9ebdcfef086c,0x800,0x100000)/File(\EFI\debian\shimx64.efi)
```

We can see that we are using boot 0003 and the shim can be found in the following folder:

```
sudo ls /boot/efi/EFI/debian
BOOTX64.CSV  fbx64.efi  grub.cfg  grubx64.efi  mmx64.efi  shimx64.efi
```

PATH: /boot/efi/EFI/debian/shimx64.efi

Q4. Verify that the shim boot loader is indeed signed with the Microsoft Corporation UEFI CA key Hint sbsigntool PEM format

Convert the certificate from .der (raw format) to .pem (plain text)

```
openssl x509 -in DB-0002.der -inform DER -out DB-0002.pem
```

Verify if the shim boot loader is signed with the certificate.

```
sudo sbverify --cert DB-0002.pem /boot/efi/EFI/debian/shimx64.efi
warning: data remaining[833960 vs 960080]: gaps between PE/COFF sections?
Signature verification OK
```

Q5. Read the first 9 pages of the specification (up to Authenticode-Specific Structures) Focus on the structure of the binaries What is the name of the part of the binary where the actual signing info is stored?

The specification shows that inside the section Attribute Certificate Table (ACT) the signing information can be found on the SignerInfos part. Which can be seen below.

```
SignerInfo ::= SEQUENCE {
  version Version,
  issuerAndSerialNumber IssuerAndSerialNumber,
  digestAlgorithm DigestAlgorithmIdentifier,
  authenticatedAttributes
    [0] IMPLICIT Attributes OPTIONAL,
  digestEncryptionAlgorithm
    DigestEncryptionAlgorithmIdentifier,
  encryptedDigest EncryptedDigest,
  unauthenticatedAttributes
    [1] IMPLICIT Attributes OPTIONAL }
IssuerAndSerialNumber ::= SEQUENCE {
  issuer Name,
  serialNumber CertificateSerialNumber }
EncryptedDigest ::= OCTET STRING
```

Q6. In what standard cryptographic format is the signature data stored?

The Cryptographic Message Syntax Standard (CMS) format is used as the standard format in which the signature data is store. The supported digestedAlgorithm are SHA1 and MD5.

Internet Engineering Task Force took over the CMS specification and this was how they described it during their introduction. “”“ This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content. Specification ”“”

Q7. Extract the signature data from the shim binary using dd Add 8 bytes to the location as given in the data directory to skip over the Microsoft WIN structure header (see page 14 of the specification if you are interested) Show the command you used

Ive installed the pev package and used the readpe for the following questions.

```
dmarque@desktop-46:~/Documents$ sudo readpe -d
/boot/efi/EFI/debian/shimx64.efi
Data directories
    Directory
        IMAGE_DIRECTORY_ENTRY_SECURITY:  0xe80a8 (9640 bytes)
    Directory
        IMAGE_DIRECTORY_ENTRY_BASERELOC: 0x82000 (10 bytes)
```

This is the entry I changed “IMAGE_DIRECTORY_ENTRY_SECURITY: 0xe80a8 (9640 bytes)” $$ 0xe80a8 + 8 = 0xE80B0 = 950448 $$

```
dmarque@desktop-46:~/Documents$ sudo dd if=/boot/efi/EFI/debian/shimx64.efi
bs=1 skip=950448 count=9632 of=shim.bin
9632+0 records in
9632+0 records out
9632 bytes (9.6 kB, 9.4 KiB) copied, 0.0243956 s, 395 kB/s
```

Which created a new file cert.pem with the content.

```
dmarque@desktop-46:~/Documents$ openssl pkcs7 -inform der -in shim.bin -
print_certs -out cert.pem of=shim.bin
dmarque@desktop-46:~/Documents$ cat cert.pem
subject=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN
= Microsoft Windows UEFI Driver Publisher
issuer=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN =
Microsoft Corporation UEFI CA 2011
-----BEGIN CERTIFICATE-----
MIIFDDCCA/SgAwIBAgITMwAAAF9GOQa5UKc57QABAAAAXzANBgkqhkiG9w0BAQsF
ADCBgTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcT
B1JlZG1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UE
AxMiTWljcm9zb2Z0IENvcnBvcmF0aW9uIFVFRkkgQ0EgMjAxMTAeFw0yMzEwMTkx
OTUzMjRaFw0yNDEwMTYxOTUzMjRaMIGGMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0
IENvcnBvcmF0aW9uMTAwLgYDVQQDEydNaWNyb3NvZnQgV2luZG93cyBVRUZJIERy
aXZlciBQdWJsaXNoZXIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDN
pMyRyq//J7apUoY/Z8QC2hYx8JjI4embB1biH9oBbEAazk/QkvzLFCoBGkbOu1M7
aSHuqf1dt+A/AXZ+aMC3Sq+0xLrZEcJxmRThZ4frLzoYm+qOHp4Sqrt4BSx0blW5
2j44XrVtSPxPHez5pAFjKqjDB0xcdL9RqNpB0znSvKiKJh627w+NnjxtSpwS4BNS
p8yDWfCMXikNLra25uPjirp5e5UQAl4OjOOBohnsGDsWEkrnYywNYzvZDnzqFvgy
0M5QGNMGw+z7b7ZKBN9EQRhuM7UQfZTC/k9PIadWUCZOWzRLMSzUY36e8uIQ8+hU
kFib2SIibGxj9daPmMSXAgMBAAGjggF0MIIBcDAfBgNVHSUEGDAWBgorBgEEAYI3
UAIBBggrBgEFBQcDAzAdBgNVHQ4EFgQUpTkmubRpUrU1YiJhbxAUHNJVGXgwRQYD
VR0RBD4wPKQ6MDgxHjAcBgNVBAsTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEWMBQG
A1UEBRMNMjI5OTExKzUwMTU5OTAfBgNVHSMEGDAWgBQTrb9DCb2CcJyM1U8xbtUi
mIob1DBWBgNVHR8ETzBNMEugSaBHhkVodHRwOi8vd3d3Lm1pY3Jvc29mdC5jb20v
cGtpb3BzL2NybC9NaWNDb3JVRUZDQTIwMTFfMjAxMS0wNi0yNy5jcmwlMjAwYAYI
KwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRwOi8vd3d3Lm1pY3Jvc29mdC5j
b20vcGtpb3BzL2NlcnRzL01pY0NvclVFRkNBMjAxMV8yMDExLTA2LTI3LmNydDAM
BgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQB6jkw9H5OCToQnKV7SQQUF
kIpL3pUzqYKMYWLIrWlbRbBkpA+oIB0rllhLY9v1J/GiBQ/ISF6BS5AZkKTxsWrX
```

```
MWVJdsG3Yq9Jxohxkt8WzIPpBX0Gd0D05X9pzz3u/BQrr4+FkBVe1OGPo2+IGmEN
iWVBGs4dJrsAc/X06AHwPr7l8qxkk5uiSIk0FhT9xijnE7eeEwjVVR/NLISOHNMk
CkQ+AdYCgCr63DdOy9iannvuAWYzrYVsXo/cEY0iL4Wlhwgnb0ysjv1HFQRJ78O7
D8Ew1mErHbKafl9GIsLeMMs2U0M4LhpOBJc/aXec0l6NHRWy/w7ci78NQQcR+fnC
-----END CERTIFICATE-----

subject=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN
= Microsoft Corporation UEFI CA 2011
issuer=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN =
Microsoft Corporation Third Party Marketplace Root
-----BEGIN CERTIFICATE-----
MIIGEDCCA/igAwIBAgIKYQjTxAAAAAAABDANBgkqhkiG9w0BAQsFADCBkTELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQx
HjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE7MDkGA1UEAxMyTWljcm9z
b2Z0IENvcnBvcmF0aW9uIFRoaXJkIFBhcnR5IE1hcmtldHBsYWNlIFJvb3QwHhcN
MTEwNjI3MjEyMjQ1WhcNMjYwNjI3MjEzMjQ1WjCBgTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vbmQxHjAcBgNVBAoTFU1p
Y3Jvc29mdCBDb3Jwb3JhdGlvbjErMCkGA1UEAxMiTWljcm9zb2Z0IENvcnBvcmF0
aW9uIFVFRkkgQ0EgMjAxMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKUIbEzHRQlqSwykwId/BnUMQwFUZOAWfwftkn0LsnO/DArGSkVhoMUWLZbT9Sug
+01Jm0GAkDy5VP3mvNGdxKQYin9BilxZg2gyu4xHye5xvCFPmop8/0Q/jY8ysiZI
rnW17slMHkoZfuSCmh14d00MsL32D9MW07z6K6VROF31+7rbeALb/+wKG5bVg7gZ
E+m2wHtAe+EfKCfJ+u9WXhzmfpR+wPBEsnk55dqyYotNvzhw4mgkFMkzpAg31Vhp
XtN87cEEUwjnTrAqh2MIYW9jFVnqsit51wxhZ4pb/V6th3+6hmdPcVgSIgQiIs6L
71RxAM5QNVh2lQjuarGiAdUCAwEAAaOCAXYwggFyMBIGCSsGAQQBgjcVAQQFAgMB
AAEwIwYJKwYBBAGCNxUCBBYEFPjBa7d/d1NK8yU3HU6hJnsPIHCAMB0GA1UdDgQW
BBQTrb9DCb2CcJyM1U8xbtUimIob1DAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMA
QTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRFZlJD
4X5YEb/WTp4jVQg7OiJqqDBcBgNVHR8EVTBTMFGgT6BNhktodHRwOi8vY3JsLm1p
Y3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNDb3JUaGlQYXJNYXJSb29f
MjAxMC0xMC0wNS5jcmwwYAYIKwYBBQUHAQEEVDBSMFAGCCsGAQUFBzAChkRodHRw
Oi8vd3d3Lm1pY3Jvc29mdC5jb20vcGtpL2NlcnRzL01pY0NvclRoaVBhck1hclJv
b18yMDEwLTEwLTA1LmNydDANBgkqhkiG9w0BAQsFAAOCAgEANQhC/zDMzvd2DK0Q
aFg1KUYydid87xJBJ0IbSqptgThIWRNV8+lYNKYWC4KqXa2C2oCDQQaPtB3yA7nz
Gl0b8VCQ+bNVhEIoHCC9sq5RFMXArJeVIRyQ2w/8d56Vc5GIyr29UrkFUA3fV56g
Ye0N5W0l2UAPF0DIzqNKwk2vmhIdCFSPvce8uSs9SSsfMvxqIWlPm8h+QjT8NgYX
i48gQMCzmiV1J83JA6P2XdHnNlR6uVC10xLRB7+7dN/cHo+A1e0Y9C8UFmsv3maM
sCPlx4TY7erBM4KtVksYLfFolQfNz/By8K673YaFmCwhTDMr8A9K8GiHtZJVMnWh
aoJqPKMlEaTtrdcErsvYQFmghNGVTGKRIhp0HYw9Rw5EpuSwmzQ1sfq2U6gsgeyk
BXHInbi66BtEZuRHVA6OVn+znxaYsobQaD6QI7UvXo9QhY3GjYJfQaH0Lg3gmdJs
deS2abUhhvoH0fbiTdHarSx3Ux4lMjfHbFJylYaw8TVhahn1sjuBUFamMi3+oon5
QoYnGFWhgspam/gwmFQUpkeWJS/IJuRBlBpcAj/lluOFWzw+P7tHFnJV4iUisdl7
5wMGKqP3HpBGwwAN1hmJ4w41J2IDcRWm79AnoKBZN2D4OJS44Hhw+LpMhoeU9uCu
AkXuZcK2o35pFnUHkpv1prxZg1g=
-----END CERTIFICATE-----
```

Q8. Show the subject and issuer of any X 509 certificates stored in the signature data

Draw a diagram relating these certificates to the Microsoft Corporation UEFI CA certificate Hint openssl strongswan-starter

```
cert#1
subject=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN
= Microsoft Windows UEFI Driver Publisher
issuer=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN =
Microsoft Corporation UEFI CA 2011

cert#2
subject=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN
= Microsoft Corporation UEFI CA 2011
issuer=C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN =
Microsoft Corporation Third Party Marketplace Root
```

Issuers Diagram

Q9. BONUS Using your new knowledge about Authenticode binaries extract the signing certificates from the GRUB boot loader and show the subject and issuer

Q10. Why is storing the certificate X in the shim binary secure?

When a certificate is stored within the shim binary modifications are not possible which means that any change on the binary signature would invalidate it. During the system boot the shim binary is checked and when there are changes found on the signature it wont boot.

Q11. What do you think is the subject CommonName (CN) of this X certificate?

I think the subject CommonName is “Debian Secure Boot Signer 2022 - grub2”.

Q12. Obtain the X certificate used by shim to verify the GRUB binary

```
sudo openssl asn1parse -i -inform DER -in /boot/efi/EFI/debian/shimx64.efi -
length 1080 -dump -offset 701514
    0:d=0  hl=2 l=  21 prim: PRINTABLESTRING   :Debian Secure Boot CA
   23:d=0  hl=2 l=  30 cons: SEQUENCE
   25:d=1  hl=2 l=  13 prim:  UTCTIME           :160816180918Z
   40:d=1  hl=2 l=  13 prim:  UTCTIME           :460809180918Z
   55:d=0  hl=2 l=  32 cons: SEQUENCE
   57:d=1  hl=2 l=  30 cons:  SET
   59:d=2  hl=2 l=  28 cons:   SEQUENCE
   61:d=3  hl=2 l=   3 prim:    OBJECT            :commonName
   66:d=3  hl=2 l=  21 prim:    PRINTABLESTRING   :Debian Secure Boot CA
   89:d=0  hl=4 l= 290 cons: SEQUENCE
   93:d=1  hl=2 l=  13 cons:  SEQUENCE
```

```
   95:d=2  hl=2 l=   9 prim:   OBJECT            :rsaEncryption
  106:d=2  hl=2 l=   0 prim:   NULL
  108:d=1  hl=4 l= 271 prim:  BIT STRING
      0000 - 00 30 82 01 0a 02 82 01-01 00 9d 95 d4 8b 9b da
.0..............
      0010 - 10 ac 2e ca 82 37 c1 a4-cb 4a c3 1b 42 93 c2 7a
.....7...J..B..z
      0020 - 29 d3 6e dd 64 af 80 af-ea 66 a2 1b 61 9c 83 0c
).n.d....f..a...
      0030 - c5 6b b9 35 25 ff c5 fb-e8 29 43 de ce 4b 3d c6
.k.5%....)C..K=.
      0040 - 12 4d b1 ef 26 43 95 68-cd 04 11 fe c2 24 9b de
.M..&C.h.....$..
      0050 - 14 d8 86 51 e8 38 43 bd-b1 9a 15 e5 08 6b f8 54
...Q.8C......k.T
      0060 - 50 8b b3 4b 5f fc 14 e4-35 50 7c 0b b1 e2 03 84
P..K_...5P|.....
      0070 - a8 36 48 e4 80 e8 ea 9f-fa bf c5 18 7b 5e ce 1c
.6H.........{^..
      0080 - be 2c 80 78 49 35 15 c0-21 cf ef 66 d5 8a 96 08
.,.xI5..!..f....
      0090 - 2b 66 2f 48 17 b1 e7 ec-82 8f 07 e6 ca e0 5f 71
+f/H.........._q
      00a0 - 24 39 50 0a 8e d1 72 28-50 a5 9d 21 f4 e3 61 ba
$9P...r(P..!..a.
      00b0 - 09 03 66 c8 df 4e 26 36-0b 15 0f 63 1f 2b af ab
..f..N&6...c.+..
      00c0 - c4 28 a2 56 64 85 8d a6-55 41 ae 3c 88 95 dd d0
.(.Vd...UA.<....
      00d0 - 6d d9 29 db d8 c4 68 b5-fc f4 57 89 6b 14 db e0
m.)...h...W.k...
      00e0 - ef ee 40 0d 62 1f ea 58-d4 a3 d8 ba 03 a6 97 2e
..@.b..X........
      00f0 - c5 6b 13 a4 91 77 a6 b5-ad 23 a7 eb 0a 49 14 46
.k...w...#...I.F
      0100 - 7c 76 e9 9e 32 b4 89 af-57 79 02 03 01 00 01
|v..2...Wy.....
  383:d=0  hl=3 l= 210 cons: cont [ 3 ]
  386:d=1  hl=3 l= 207 cons:  SEQUENCE
  389:d=2  hl=2 l=  65 cons:   SEQUENCE
  391:d=3  hl=2 l=   8 prim:    OBJECT            :Authority Information
Access
  401:d=3  hl=2 l=  53 prim:    OCTET STRING
      0000 - 30 33 30 31 06 08 2b 06-01 05 05 07 30 02 86 25
0301..+.....0..%
      0010 - 68 74 74 70 73 3a 2f 2f-64 73 61 2e 64 65 62 69
https://dsa.debi
      0020 - 61 6e 2e 6f 72 67 2f 73-65 63 75 72 65 2d 62 6f
an.org/secure-bo
```

```
      0030 - 6f 74 2d 63 61                                    ot-ca
  456:d=2  hl=2 l=  31 cons:   SEQUENCE
  458:d=3  hl=2 l=   3 prim:    OBJECT            :X509v3 Authority Key
Identifier
  463:d=3  hl=2 l=  24 prim:    OCTET STRING
      0000 - 30 16 80 14 6c ce ce 7e-4c 6c 0d 1f 61 49 f3 dd
0...l..~Ll..aI..
      0010 - 27 df cc 5c bb 41 9e a1-                          '..\.A..
  489:d=2  hl=2 l=  20 cons:   SEQUENCE
  491:d=3  hl=2 l=   9 prim:    OBJECT            :Netscape Cert Type
  502:d=3  hl=2 l=   1 prim:    BOOLEAN           :255
  505:d=3  hl=2 l=   4 prim:    OCTET STRING
      0000 - 03 02 00 f7                                       ....
  511:d=2  hl=2 l=  19 cons:   SEQUENCE
  513:d=3  hl=2 l=   3 prim:    OBJECT            :X509v3 Extended Key Usage
  518:d=3  hl=2 l=  12 prim:    OCTET STRING
      0000 - 30 0a 06 08 2b 06 01 05-05 07 03 03               0...+.......
  532:d=2  hl=2 l=  14 cons:   SEQUENCE
  534:d=3  hl=2 l=   3 prim:    OBJECT            :X509v3 Key Usage
  539:d=3  hl=2 l=   1 prim:    BOOLEAN           :255
  542:d=3  hl=2 l=   4 prim:    OCTET STRING
      0000 - 03 02 01 86                                       ....
  548:d=2  hl=2 l=  15 cons:   SEQUENCE
  550:d=3  hl=2 l=   3 prim:    OBJECT            :X509v3 Basic Constraints
  555:d=3  hl=2 l=   1 prim:    BOOLEAN           :255
  558:d=3  hl=2 l=   5 prim:    OCTET STRING
      0000 - 30 03 01 01 ff                                    0....
  565:d=2  hl=2 l=  29 cons:   SEQUENCE
  567:d=3  hl=2 l=   3 prim:    OBJECT            :X509v3 Subject Key
Identifier
  572:d=3  hl=2 l=  22 prim:    OCTET STRING
      0000 - 04 14 6c ce ce 7e 4c 6c-0d 1f 61 49 f3 dd 27 df
..l..~Ll..aI..'.
      0010 - cc 5c bb 41 9e a1                                 .\.A..
  596:d=0  hl=2 l=  13 cons: SEQUENCE
  598:d=1  hl=2 l=   9 prim:  OBJECT            :sha256WithRSAEncryption
  609:d=1  hl=2 l=   0 prim:  NULL
  611:d=0  hl=4 l= 257 prim: BIT STRING
      0000 - 00 77 96 3e 47 c9 ce 09-cf 8b 89 ce 59 ed 26 0e
.w.>G.......Y.&.
      0010 - 26 0b b9 ad a9 2b bd a1-eb 88 79 02 ff 31 de fe
&....+....y..1..
      0020 - f5 6a 07 ef 61 13 11 70-1e bf 9c 4e 66 6c e1 62
.j..a..p...Nfl.b
      0030 - 12 97 01 57 65 47 dd 4a-c6 f7 f4 de a8 f1 13 62
...WeG.J.......b
      0040 - cc 83 57 ac 3c a6 91 15-af 55 26 72 69 2e 14 cd
..W.<....U&ri...
      0050 - dd 4d b3 d1 60 24 2d 32-4f 19 6c 11 5e f2 a3 f2
.M..`$-2O.l.^...
      0060 - a1 5f 62 0f 30 ae ad f1-48 66 64 7d 36 44 0d 06
```

```
._b.0...Hfd}6D..
      0070 - 34 3d 2e af 8e 9d c3 ad-c2 91 d8 37 e0 ee 7a 5f
4=.........7..z_
      0080 - 82 3b 67 8e 00 8a c4 a4-df 35 16 c2 72 2b 4c 51
.;g......5..r+LQ
      0090 - d7 93 93 9e ba 08 0d 59-97 f2 e2 29 a0 44 4d ea
.......Y...).DM.
      00a0 - ee f8 3e 02 60 ca 15 cf-4e 9a 25 91 84 3f b7 5a
..>.`...N.%..?.Z
      00b0 - c7 ee bc 6b 80 a3 d9 fd-b2 6d 7a 1e 63 14 eb ef
...k.....mz.c...
      00c0 - f1 b0 40 25 d5 e8 0e 81-eb 6b f7 cb ff e5 21 00
..@%.....k....!.
      00d0 - 22 2c 2e 9a 35 60 12 4b-5b 5f 38 46 84 0c 06 9c
",..5`.K[_8F....
      00e0 - cf 72 93 62 18 ee 5c 98-d6 b3 7d 06 25 39 95 df
.r.b..\...}.%9..
      00f0 - 4e 60 76 b0 06 7b 08 b0-6e e3 64 9f 21 56 ad 39
N`v..{..n.d.!V.9
      0100 - 0f                                               .
  872:d=0  hl=2 l=  22 cons: OBJECT
Error in encoding
40A7E5C77F7F0000:error:0680007B:asn1 encoding
routines:ASN1_get_object:header too long:../crypto/asn1/asn1_lib.c:105:
```

The last SEQUENCE is the same as the following certificate:

```
SHA1 Fingerprint:
53:61:0c:f8:1f:bd:7e:0c:eb:67:91:3c:9e:f3:e7:94:a9:63:3e:cb
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ed:54:a1:d5:af:87:48:94:8d:9f:89:32:ee:9c:7c:34
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Debian Secure Boot CA
        Validity
            Not Before: Aug 16 18:09:18 2016 GMT
            Not After : Aug  9 18:09:18 2046 GMT
        Subject: CN=Debian Secure Boot CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9d:95:d4:8b:9b:da:10:ac:2e:ca:82:37:c1:a4:
                    cb:4a:c3:1b:42:93:c2:7a:29:d3:6e:dd:64:af:80:
                    af:ea:66:a2:1b:61:9c:83:0c:c5:6b:b9:35:25:ff:
                    c5:fb:e8:29:43:de:ce:4b:3d:c6:12:4d:b1:ef:26:
                    43:95:68:cd:04:11:fe:c2:24:9b:de:14:d8:86:51:
```

```
                    e8:38:43:bd:b1:9a:15:e5:08:6b:f8:54:50:8b:b3:
                    4b:5f:fc:14:e4:35:50:7c:0b:b1:e2:03:84:a8:36:
                    48:e4:80:e8:ea:9f:fa:bf:c5:18:7b:5e:ce:1c:be:
                    2c:80:78:49:35:15:c0:21:cf:ef:66:d5:8a:96:08:
                    2b:66:2f:48:17:b1:e7:ec:82:8f:07:e6:ca:e0:5f:
                    71:24:39:50:0a:8e:d1:72:28:50:a5:9d:21:f4:e3:
                    61:ba:09:03:66:c8:df:4e:26:36:0b:15:0f:63:1f:
                    2b:af:ab:c4:28:a2:56:64:85:8d:a6:55:41:ae:3c:
                    88:95:dd:d0:6d:d9:29:db:d8:c4:68:b5:fc:f4:57:
                    89:6b:14:db:e0:ef:ee:40:0d:62:1f:ea:58:d4:a3:
                    d8:ba:03:a6:97:2e:c5:6b:13:a4:91:77:a6:b5:ad:
                    23:a7:eb:0a:49:14:46:7c:76:e9:9e:32:b4:89:af:
                    57:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:https://dsa.debian.org/secure-boot-ca
            X509v3 Authority Key Identifier:
                6C:CE:CE:7E:4C:6C:0D:1F:61:49:F3:DD:27:DF:CC:5C:BB:41:9E:A1
            Netscape Cert Type: critical
                SSL Client, SSL Server, S/MIME, Object Signing, SSL CA,
S/MIME CA, Object Signing CA
            X509v3 Extended Key Usage:
                Code Signing
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                6C:CE:CE:7E:4C:6C:0D:1F:61:49:F3:DD:27:DF:CC:5C:BB:41:9E:A1
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        77:96:3e:47:c9:ce:09:cf:8b:89:ce:59:ed:26:0e:26:0b:b9:
        ad:a9:2b:bd:a1:eb:88:79:02:ff:31:de:fe:f5:6a:07:ef:61:
        13:11:70:1e:bf:9c:4e:66:6c:e1:62:12:97:01:57:65:47:dd:
        4a:c6:f7:f4:de:a8:f1:13:62:cc:83:57:ac:3c:a6:91:15:af:
        55:26:72:69:2e:14:cd:dd:4d:b3:d1:60:24:2d:32:4f:19:6c:
        11:5e:f2:a3:f2:a1:5f:62:0f:30:ae:ad:f1:48:66:64:7d:36:
        44:0d:06:34:3d:2e:af:8e:9d:c3:ad:c2:91:d8:37:e0:ee:7a:
        5f:82:3b:67:8e:00:8a:c4:a4:df:35:16:c2:72:2b:4c:51:d7:
        93:93:9e:ba:08:0d:59:97:f2:e2:29:a0:44:4d:ea:ee:f8:3e:
        02:60:ca:15:cf:4e:9a:25:91:84:3f:b7:5a:c7:ee:bc:6b:80:
        a3:d9:fd:b2:6d:7a:1e:63:14:eb:ef:f1:b0:40:25:d5:e8:0e:
        81:eb:6b:f7:cb:ff:e5:21:00:22:2c:2e:9a:35:60:12:4b:5b:
        5f:38:46:84:0c:06:9c:cf:72:93:62:18:ee:5c:98:d6:b3:7d:
        06:25:39:95:df:4e:60:76:b0:06:7b:08:b0:6e:e3:64:9f:21:
        56:ad:39:0f
```

Or using the previous commands for the other questions.

```
dmarque@desktop-46:~/Documents$ sudo readpe -d
/boot/efi/EFI/debian/grubx64.efi
Data directories
    Directory
        IMAGE_DIRECTORY_ENTRY_SECURITY:  0x401000 (1472 bytes)
    Directory
        IMAGE_DIRECTORY_ENTRY_BASERELOC: 0x400000 (4096 bytes)
```

```
dmarque@desktop-46:~/Documents$ sudo dd if=/boot/efi/EFI/debian/grubx64.efi
bs=1 skip=$((0x401000 + 8)) count=1472 of=grub.bin
1464+0 records in
1464+0 records out
1464 bytes (1.5 kB, 1.4 KiB) copied, 0.00523165 s, 280 kB/s
```

Here is the certificate

```
dmarque@desktop-46:~/Documents$ sudo openssl pkcs7 -inform der -in grub.bin
-print_certs  -out grub_cert.pem
subject=CN = Debian Secure Boot Signer 2022 - grub2
issuer=CN = Debian Secure Boot CA
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIUMqAof4QaA2+jk8HgZcQ65rJCJkIwDQYJKoZIhvcNAQEL
BQAwIDEeMBwGA1UEAxMVRGViaWFuIFNlY3VyZSBCb290IENBMB4XDTIyMDgxODE3
MzIzNFoXDTMyMDgxNTE3MzIzNFowMTEvMC0GA1UEAwwmRGViaWFuIFNlY3VyZSBC
b290IFNpZ25lciAyMDIyIC0gZ3J1YjIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC/dZ/eNnOo+3NlyaddrZ8ERJWJmx4iiiLm1NeaTZByLCykiqFZ3pvE
L5xIdXb4Eegf/sGocds1/WtmocxDGuY9fO+o+drnJNUVXDw2e6bVifhGvz1uj+v9
Ct5Dwd1/slC3ciSEy9n6G4fKlc5yTdMifSarm3goahQoBudqXtDVdVM5KxL36sYS
RX09Nmtf/vnWpCqACDVrz+R5Cp8phiwpbcpE/CesTWrl9RdYk3Bs6fPAlf9Vp7QC
ToUr7TqWodxEr30Az/vMiEWX8PdSDA7TnzNYm4xNOML24mGCajE0FsKKZ11yi1JO
IGfbp9voLoPa2D9+QKx70s4BCDKIwMkxAgMBAAGjZDBiMAsGA1UdDwQEAwIHgDAT
BgNVHSUEDDAKBggrBgEFBQcDAzAdBgNVHQ4EFgQUDIc5Fy0WOBdf56A7KoQr5qKH
lTowHwYDVR0jBBgwFoAUbM7OfkxsDR9hSfPdJ9/MXLtBnqEwDQYJKoZIhvcNAQEL
BQADggEBAD7Y8/ztOUEWZmUr/08VRqkLZMnAZ2b9lbyZYbBCdlweH90ydVgnemZb
RnGTDfSbJKoKFIyQsxOcrn/Yz4PTp+6zeCqRhXrEybe22ZLzIJ29CKa+uaOqyE2i
1o9lSyAuvCAS0w5TwjBNBJwY5vYkoiQgLCcbNiXYWkeqaDEFFUFFOlNxLsfec/FH
9Dxd5j3H/hMqmvvYksTDuovVsiYvzpV1aCq/8H6Tte7SS5cJwLQhML8mU/p9EjwX
Axk5isggit+OsHlLAxlTFfkT4GHhVcYoZiAT+7sGQMghBIOWIpU3tljMJzNHrcH4
ewBsb4YPcT3DNhAMyqL+BxM79OgIlow=
-----END CERTIFICATE-----
```

Q13. Verify that this X certificate's corresponding private key was indeed used to sign the GRUB binary

```
dmarque@desktop-46:~/Documents$ sudo sbverify --cert grub_cert.pem
/boot/efi/EFI/debian/grubx64.efi
```

```
Signature verification OK
```

Q14. Verify the kernel you booted against the X certificate

Q15. BONUS Where does GRUB get its trusted certificate from? Hint It is not stored in the binary and it is not stored on the file system

Q16. Draw a diagram that shows the chain of trust from the UEFI PK key to the signed kernel Show all certificates binaries and signing relations involved