

SN LAB ASSIGNMENT: UEFI SECURE BOOT

27 OCT. 2016

ALI ABDULMADZHIDOV

2. Firmware databases

1. 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.

SHA1 Fingerprint: 46:de:f6:3b:5c:e6:1c:f8:ba:0d:e2:e6:63:9c:10:19:d0:ed:14:f3
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:

keyid: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

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`

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

Root certificate is Platform Key.

PK (platform key - could be single key or database) needed for checking updates for KEK. Only signed with PK updates can be uploaded to KEK databases. By default comes from OEM.

```
PK: List 0, type X509
Signature 0, size 1435, owner f5a96b31-dba0-4faa-2aa4-7a0c9832768e
Subject:
    O=Hewlett-Packard Company, OU=Long Lived CodeSigning Certificate,
CN=Hewlett-Packard UEFI Secure Boot Platform Key
Issuer:
    C=US, O=Hewlett-Packard Company, CN=Hewlett-Packard Printing Device
Infrastructure CA
```

3. SHIM

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

On the 9th line of efibootmgr output we can see, that ubuntu OS is loading via \EFI\ubuntu\shimx64.efi

```
→ ~ efibootmgr -v

BootCurrent: 0000

Timeout: 0 seconds

BootOrder: 0000,0001,0002,0003,0009,000A,0006,0005

Boot0000* ubuntuHD(1,GPT,43442116-14d5-46dc-8bf2-
a1831dc53be7,0x800,0x100000)/File(\EFI\ubuntu\shimx64.efi)

Boot0001* DT0 UEFI USB Floppy/CDVenMedia(b6fef66f-1495-4584-a836-
3492d1984a8d,0500000001)..B0

Boot0002* DT0 UEFI USB Hard DriveVenMedia(b6fef66f-1495-4584-a836-
3492d1984a8d,0200000001)..B0

Boot0003* DT0 UEFI ATAPI CD-ROM DriveVenMedia(b6fef66f-1495-4584-a836-
3492d1984a8d,0300000001)..B0

Boot0005 DT0 Legacy USB Floppy/CDVenMedia(b6fef66f-1495-4584-a836-
3492d1984a8d,0500000000)..B0

Boot0006 Hard DriveBBS(HD,,0x0)..GO..NO?.....F.a.k.e. .U.s.b.
.O.p.t.i.o.n.....B0

Boot0009* IP4 Intel(R) Ethernet Connection I217-
LMPciRoot(0x0)/Pci(0x19,0x0)/MAC(ecb1d7387f87,0)/IPv4(0.0.0.0:<-
>0.0.0.0:0,0,0)..B0

Boot000A* IP6 Intel(R) Ethernet Connection I217-
LMPciRoot(0x0)/Pci(0x19,0x0)/MAC(ecb1d7387f87,0)/IPv6([::]:<->
[::]:,0,0)..B0
```

4. Verify that the 'shim' boot loader is indeed signed with the 'Microsoft Corporation UEFI CA' key.

Firstly we should take out Microsoft Corporation UEFI CA and convert them to pem format.

It's easier to do via python script, that i wrote for that.

Firstly we walk through shimx64.efi, to find all certificates.

```
1 ~ → sh binwalk shimx64.efi
2
3 DECIMAL          HEXADECIMAL      DESCRIPTION
4 -----
5 0                0x0          Microsoft executable, portable (PE)
6 75931            0x1289B       mcrypt 2.2 encrypted data, algorithm:
    blowfish-448, mode: CBC, keymode: 8bit
7 751040           0xB75C0       SHA256 hash constants, little endian
8 781251           0xBEBC3       Ubiquiti firmware header, third party,
    ~CRC32: 0x10000, version: "SSL_init"
9 807162           0xC50FA       Unix path: /usr/local/ssl/private
10 808128           0xC54C0       Unix path: /usr/local/ssl/lib/engines
11 818688           0xC7E00       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 924
12 923264           0xE1680       Base64 standard index table
13 931344           0xE3610       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 1076
14 1159455          0x11B11F       mcrypt 2.2 encrypted data, algorithm:
    blowfish-448, mode: CBC, keymode: 8bit
15 1280941          0x138BAD       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 1316
16 1282261          0x1390D5       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 1552
17 1284166          0x139846       Unix path:
    /www.microsoft.com/whdc/hcl/default.msp#0
18 1284873          0x139B09       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 1649
19 1286526          0x13A17E       Certificate in DER format (x509 v3),
    header length: 4, sequence length: 1242
```

Then we, using offsets and length of certificates, take them out with dd and convert with openssl.

```
1 from bash import bash
2
3 c = {"818688": "928", "931344": "1080", "1280941": "1320",
    "1282261": "1556", "1284873": "1653", "1286526": "1248"}
4 for a,b in c.iteritems():
5     b = bash("dd if=shimx64.efi bs=1 skip="+a+" count="+b + "
    of="+a+".der")
6     print b.stdout + " | " + b.stderr
7     n = bash("openssl x509 -inform der -in " + a + ".der -text > " + a +
    ".pem")
8
9
```

Now we can find needed "Microsoft Corporation UEFI CA 2011" and try to verify shim with it.

```
1 → sh sbverify --cert 1282261.txt shimx64.efi
2 warning: data remaining[1170360 vs 1289424]: gaps between PE/COFF
  sections?
3 Signature verification OK
4
5 → sh cat 1282261.txt
6 Certificate:
7   Data:
8     Version: 3 (0x2)
9     Serial Number:
10      61:08:d3:c4:00:00:00:00:00:04
11    Signature Algorithm: sha256WithRSAEncryption
12    Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
  CN=Microsoft Corporation Third Party Marketplace Root
13    Validity
14      Not Before: Jun 27 21:22:45 2011 GMT
15      Not After : Jun 27 21:32:45 2026 GMT
16    Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
  CN=Microsoft Corporation UEFI CA 2011
17 ...
18 ...
```

5. In SignedData structure

6. RSA with SHA-256

7. I took it out in 4th question

8.

```
Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation Third Party Marketplace Root
Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation,
CN=Microsoft Corporation UEFI CA 2011
```

9. Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=GB, ST=Isle of Man, L=Douglas, O=Canonical Ltd.,
CN=Canonical Ltd. Master Certificate Authority
Validity
Not Before: Apr 12 11:39:08 2012 GMT
Not After : Apr 11 11:39:08 2042 GMT
Subject: C=GB, ST=Isle of Man, O=Canonical Ltd., OU=Secure Boot,
CN=Canonical Ltd. Secure Boot Signing
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:c9:5f:9b:62:8f:0b:b0:64:82:ac:be:c9:e2:62:
e3:4b:d2:9f:1e:8a:d5:61:1a:2b:5d:38:f4:b7:ce:
b9:9a:b8:43:b8:43:97:77:ab:4f:7f:0c:70:46:0b:
fc:7f:6d:c6:6d:ea:80:5e:01:d2:b7:66:1e:87:de:
0d:6d:d0:41:97:a8:a5:af:0c:63:4f:f7:7c:c2:52:
cc:a0:31:a9:bb:89:5d:99:1e:46:6f:55:73:b9:76:
69:ec:d7:c1:fc:21:d6:c6:07:e7:4f:bd:22:de:e4:
a8:5b:2d:db:95:34:19:97:d6:28:4b:21:4c:ca:bb:
1d:79:a6:17:7f:5a:f9:67:e6:5c:78:45:3d:10:6d:
b0:17:59:26:11:c5:57:e3:7f:4e:82:ba:f6:2c:4e:
c8:37:4d:ff:85:15:84:47:e0:ed:3b:7c:7f:bc:af:
e9:01:05:a7:0c:6f:c3:e9:8d:a3:ce:be:a6:e3:cd:
3c:b5:58:2c:9e:c2:03:1c:60:22:37:39:ff:41:02:
c1:29:a4:65:51:ff:33:34:aa:42:15:f9:95:78:fc:
2d:f5:da:8a:85:7c:82:9d:fb:37:2c:6b:a5:a8:df:
7c:55:0b:80:2e:3c:b0:63:e1:cd:38:48:89:e8:14:
06:0b:82:bc:fd:d4:07:68:1b:0f:3e:d9:15:dd:94:
11:1b
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Extended Key Usage:
Code Signing, 1.3.6.1.4.1.311.10.3.6
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
61:48:2A:A2:83:0D:0A:B2:AD:5A:F1:0B:72:50:DA:90:33:DD:CE:F0
X509v3 Authority Key Identifier:

keyid:AD:91:99:0B:C2:2A:B1:F5:17:04:8C:23:B6:65:5A:26:8E:34:5A:63

Signature Algorithm: sha256WithRSAEncryption
8f:8a:a1:06:1f:29:b7:0a:4a:d5:c5:fd:81:ab:25:ea:c0:7d:
e2:fc:6a:96:a0:79:93:67:ee:05:0e:25:12:25:e4:5a:f6:aa:
1a:f1:12:f3:05:8d:87:5e:f1:5a:5c:cb:8d:23:73:65:1d:15:
b9:de:22:6b:d6:49:67:c9:a3:c6:d7:62:4e:5c:b5:f9:03:83:

40:81:dc:87:9c:3c:3f:1c:0d:51:9f:94:65:0a:84:48:67:e4:
a2:f8:a6:4a:f0:e7:cd:cd:bd:94:e3:09:d2:5d:2d:16:1b:05:
15:0b:cb:44:b4:3e:61:42:22:c4:2a:5c:4e:c5:1d:a3:e2:e0:
52:b2:eb:f4:8b:2b:dc:38:39:5d:fb:88:a1:56:65:5f:2b:4f:
26:ff:06:78:10:12:eb:8c:5d:32:e3:c6:45:af:25:9b:a0:ff:
8e:ef:47:09:a3:e9:8b:37:92:92:69:76:7e:34:3b:92:05:67:
4e:b0:25:ed:bc:5e:5f:8f:b4:d6:ca:40:ff:e4:e2:31:23:0c:
85:25:ae:0c:55:01:ec:e5:47:5e:df:5b:bc:14:33:e3:c6:f5:
18:b6:d9:f7:dd:b3:b4:a1:31:d3:5a:5c:5d:7d:3e:bf:0a:e4:
e4:e8:b4:59:7d:3b:b4:8c:a3:1b:b5:20:a3:b9:3e:84:6f:8c:
21:00:c3:39

-----BEGIN CERTIFICATE-----

MIIEIDCCAwigAwIBAgIBATANBgkqhkiG9w0BAQsFADCbHDELMakGA1UEBhMCR0Ix
FDASBgNVBAGMC0lzbGUgb2YgTWFuMRAwDgYDVQQHDAEb3VnbGFzMRCwFQYDVQQK
DA5DYW5vbmljYWwgTHRkLjE0MDIGA1UEAwwrQ2Fub25pY2FsIEx0ZC4gTWfzdGVy
IENlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0xMjA0MTIxMTM5MDhaFw00MjA0MTEx
MTM5MDhaMH8xCzAJBgNVBAYTAkdCMRQwEgYDVQQIDAtJc2x1IG9mIE1hbjEXMBUG
A1UECgw0Q2Fub25pY2FsIEx0ZC4xFDASBgNVBASMC1NlY3VyZSBcb290MSswKQYD
VQDDCJDYw5vbmljYWwgTHRkLiBTZW51cmUgQm9vdCBTaWduaW5nMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYV+bYo8LsGSCrL7J4mLjS9KfHorVYRor
XTj0t865mrhDuEOXd6tPfwxwRgv8f23GbeqAXgHSt2Yeh94NbdBB16ilrwxjT/d8
wLLMoDGpu4ldmR5Gb1VzuXZp7NfB/CHWxgfnT70i3uSowY3b1TQZl9YoSyFMyrsd
eaYXf1r5Z+ZceEU9EG2wF1kmEcVX4390grr2LE7IN03/hRWER+Dt03x/vK/pAQWn
DG/D6Y2jzr6m4808tVgsnsIDHGAiNzn/QQLBKarluf8zNKpCFfmVePwt9dqKhXyC
nfs3LGulqN98VQuALjyWY+HN0EiJ6BQGC4K8/dQHaBsPPtkV3ZQRGwIDAQAB04Gg
MIGdMAwGA1UdEwEB/wQCMAAwHwYDVR0lBBGwFgYIKwYBBQUHAWMGcisGAQQBgjck
AwYwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRl
MB0GA1UdDgQWBBRhSCqigw0Ksq1a8QtYUNqQM9308DAfBgNVHSMEGDAWgBStkZkL
wiqx9RcEjC02ZVomjjRaYzANBgkqhkiG9w0BAQsFAAOCAQEaj4qhBh8ptwpK1cX9
gasl6sB94vxqlqB5k2fuBQ4lEiXkwvaqGvES8wWNh17xwLzLjSNzZR0Vud4ia9ZJ
Z8mjxtDiTly1+Q0DQIHch5w8PwxNUZ+UZQqESGfkovimSvDnzc29l0MJ0l0tFhsF
FQvLRLQ+YUIixCpcTsUdo+LgUrLr9Isr3Dg5XfuIoVZlXytPJv8GeBAS64xdMuPG
Ra8lm6D/ju9HCaPpizeSkml2fjQ7kgVnTrAl7bxeX4+01spA/+TiMSMMhSWuDFUB
70VHXt9bvBQz48b1GLbZ992ztKEx01pcXX0+vwrk50i0WX07tIyjG7Ugo7k+hG+M
IQDDOQ==

-----END CERTIFICATE-----

10. Because any changes in it, without signing with Microsoft UEFI CA key would be detected, and secure boot wouldn't load it
11. CN=Canonical Ltd. Master Certificate Authority.
12. I have obtained them all in 4th question.


```

13. → sh sbverify --cert 931344.txt grubx64.efi
Signature verification OK
→ sh cat 931344.txt
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 13348991040521802343 (0xb94124a0182c9267)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=GB, ST=Isle of Man, L=Douglas, O=Canonical Ltd.,
CN=Canonical Ltd. Master Certificate Authority
  Validity
    Not Before: Apr 12 11:12:51 2012 GMT
    Not After : Apr 11 11:12:51 2042 GMT
  Subject: C=GB, ST=Isle of Man, L=Douglas, O=Canonical Ltd.,
CN=Canonical Ltd. Master Certificate Authority
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:bf:5b:3a:16:74:ee:21:5d:ae:61:ed:9d:56:ac:
      bd:de:de:72:f3:dd:7e:2d:4c:62:0f:ac:c0:6d:48:
      08:11:cf:8d:8b:fb:61:1f:27:cc:11:6e:d9:55:3d:
      39:54:eb:40:3b:b1:bb:e2:85:34:79:ca:f7:7b:bf:
      ba:7a:c8:10:2d:19:7d:ad:59:cf:a6:d4:e9:4e:0f:
      da:ae:52:ea:4c:9e:90:ce:c6:99:0d:4e:67:65:78:
      5d:f9:d1:d5:38:4a:4a:7a:8f:93:9c:7f:1a:a3:85:
      db:ce:fa:8b:f7:c2:a2:21:2d:9b:54:41:35:10:57:
      13:8d:6c:bc:29:06:50:4a:7e:ea:99:a9:68:a7:3b:
      c7:07:1b:32:9e:a0:19:87:0e:79:bb:68:99:2d:7e:
      93:52:e5:f6:eb:c9:9b:f9:2b:ed:b8:68:49:bc:d9:
      95:50:40:5b:c5:b2:71:aa:eb:5c:57:de:71:f9:40:
      0a:dd:5b:ac:1e:84:2d:50:1a:52:d6:e1:f3:6b:6e:
      90:64:4f:5b:b4:eb:20:e4:61:10:da:5a:f0:ea:e4:
      42:d7:01:c4:fe:21:1f:d9:b9:c0:54:95:42:81:52:
      72:1f:49:64:7a:c8:6c:24:f1:08:70:0b:4d:a5:a0:
      32:d1:a0:1c:57:a8:4d:e3:af:a5:8e:05:05:3e:10:
      43:a1
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      AD:91:99:0B:C2:2A:B1:F5:17:04:8C:23:B6:65:5A:26:8E:34:5A:63
    X509v3 Authority Key Identifier:

keyid:AD:91:99:0B:C2:2A:B1:F5:17:04:8C:23:B6:65:5A:26:8E:34:5A:63

    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 Key Usage:
      Digital Signature, Certificate Sign, CRL Sign
    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://www.canonical.com/secure-boot-master-ca.crl

```

Signature Algorithm: sha256WithRSAEncryption

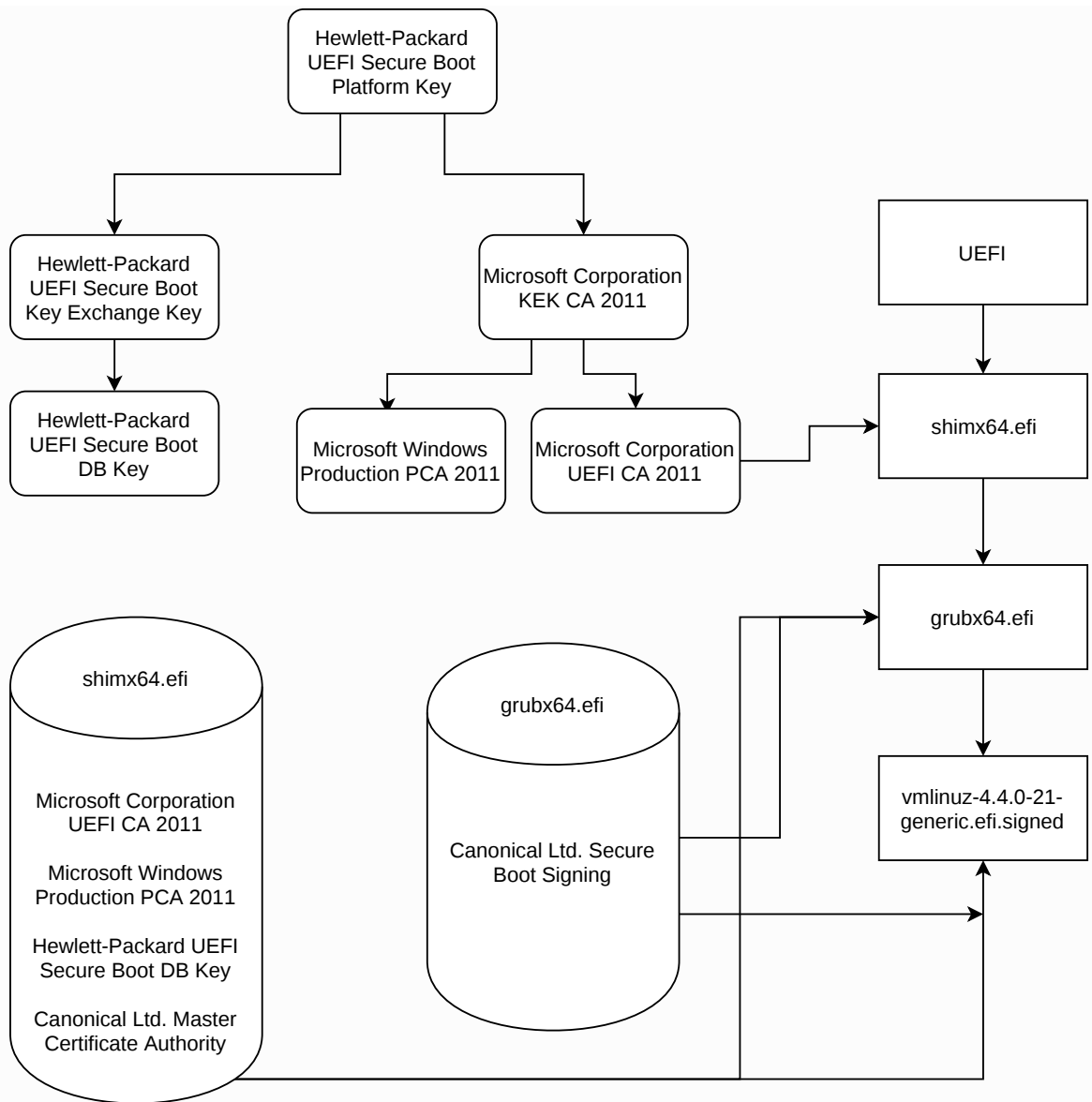
```
3f:7d:f6:76:a5:b3:83:b4:2b:7a:d0:6d:52:1a:03:83:c4:12:
a7:50:9c:47:92:cc:c0:94:77:82:d2:ae:57:b3:99:04:f5:32:
3a:c6:55:1d:07:db:12:a9:56:fa:d8:d4:76:20:eb:e4:c3:51:
db:9a:5c:9c:92:3f:18:73:da:94:6a:a1:99:38:8c:a4:88:6d:
c1:fc:39:71:d0:74:76:16:03:3e:56:23:35:d5:55:47:5b:1a:
1d:41:c2:d3:12:4c:dc:ff:ae:0a:92:9c:62:0a:17:01:9c:73:
e0:5e:b1:fd:bc:d6:b5:19:11:7a:7e:cd:3e:03:7e:66:db:5b:
a8:c9:39:48:51:ff:53:e1:9c:31:53:91:1b:3b:10:75:03:17:
ba:e6:81:02:80:94:70:4c:46:b7:94:b0:3d:15:cd:1f:8e:02:
e0:68:02:8f:fb:f9:47:1d:7d:a2:01:c6:07:51:c4:9a:cc:ed:
dd:cf:a3:5d:ed:92:bb:be:d1:fd:e6:ec:1f:33:51:73:04:be:
3c:72:b0:7d:08:f8:01:ff:98:7d:cb:9c:e0:69:39:77:25:47:
71:88:b1:8d:27:a5:2e:a8:f7:3f:5f:80:69:97:3e:a9:f4:99:
14:db:ce:03:0e:0b:66:c4:1c:6d:bd:b8:27:77:c1:42:94:bd:
fc:6a:0a:bc
```

-----BEGIN CERTIFICATE-----

```
MIIENDCCAxgAwIBAgIJALlBJKAYLJJnMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
VQQGEwJHqjEUMBIGA1UECAwLSXNsZSBvZiBNYW4xEDA0BgNVBACMB0RvdWdsYXMX
FzAVBgNVBAOMdKNhbm9uawNhbCBMdGQuMTQwMgYDVQQDDCtDYW5vbmljYWwgTHRk
LiBNYXN0ZXIgaQ2VydGlmawNhdGUgQXV0aG9yaXR5MB4XDTEyMTI1MVVoX
DTQyMDQxMTExMTI1MVowgYQxCzAJBgNVBAYTAkdCMRQwEgYDVQQIDAtJc2x1IG9m
IE1hbGjEQMA4GA1UEBwwHRG91Z2xhc2EXMBUGA1UECgwOQ2Fub25pY2FsIEEx0ZC4x
NDAYBgNVBAMMK0Nhb9uawNhbCBMdGQuIE1hc3RlcjB0ZXJ0aWZpY2F0ZSBBDXR0
b3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC/WzoWd04hXa5h
7Z1WrL3e3nLz3X4tTGIPrMBtSAGRz42L+2EfJ8wRbt1VPT1U60A7sbvihTR5yvd7
v7p6yBAtGX2tWc+m10l0D9quUupMnpD0xpKNTmdleF350dU4Sklp6j50cfxqjhdv0
+ov3wqIhLZtUQTUQVxONbLwpBlBKfuqZqWin08cHGzKeoBmHDnm7aJktfpNS5fbr
yZv5K+24aEm82ZVQqFvFsnGq61xX3nH5QArDw6wehC1QG1LW4fNrbpBkT1u06yDk
YRDawvDq5ELXAct+IR/ZucBUlUKBUnIfSWR6yGwk8QhwC02loDLRoBxXqE3jr6W0
BQU+EE0hAgMBAAGjgaYwgaMwHQYDVR00BBYEFK2RmQvCKrH1FwSMI7Z1Wia0NFpj
MB8GA1UdIwQYMBAAAFK2RmQvCKrH1FwSMI7Z1Wia0NFpjMA8GA1UdEwEB/wQFMAMB
Af8wCwYDVR0PBAQDAgGGMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly93d3cuY2Fu
b25pY2FsLmNvbS9zZWN1cmUtYm9vdC1tYXN0ZXItY2EuY3JsMA0GCSqGSIb3DQEB
CwUAA4IBAQA/ffZ2pb0DtCt60G1SGg0DxBKnUJxHksZAlHeC0q5Xs5kE9TI6x1Ud
B9sSqVb62NR2IOvkw1Hbmlyckj8Yc9qUaqGZOIykiG3B/Dlx0HR2FgM+ViM11VVH
WxodQcLTEkzc/64KkpxiChcBnHPgXrH9vNa1GRF6fs0+A35m21uoyTlIUf9T4Zwx
U5Eb0xB1Axe65oECgJRwTEa3lLA9Fc0fjgLgaAKP+/lHHX2iAcYHUcSaz03dz6Nd
7ZK7vtH95uwfM1FzBL48crB9CPgB/5h9y5zgaTl3JUdxilGNJ6UuqPc/X4Bplz6p
9JkU284DDgtmxBxtvbgnd8FC1L38agq8
-----END CERTIFICATE-----
```

14.

```
→ sh sbverify --cert 931344.txt vmlinuz-4.4.0-21-generic.efi.signed
Signature verification OK
```



15.