Read ssh key with openssl command in CLI

593 Nesvin KN March 24, 2025 General 9260

How to read SSH key with OpenSSL CLI command?

Overview: This article explains how to read an SSH private key using the OpenSSL CLI command.

Step 1: Run below command to find if the key is readable from the command line of the Linux server.

root@linux_server:~# openssl pkey -in {path_to_any_private_key} -pubout -text

Example for readable key in the Linux server.:

root@linux_server:~# openssl pkey -in .ssh/id_rsa -pubout -text

-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAyu9c192+qbAg4d41fgiQ
I6HQ3AVsTI6kBufctn22WHjS/WlrOgqR15HcKf2UGeWjjoBX+px6ban/VZZbD+EO
EDlgoLP9zpay7ymQI8ssdqjbABVS2RDC1LZg+cSB1d0PXx8bfnm3LcokcsUPRGFp
oHCPeRhWEpBt+rYHN3CEhCFzrcIUIarPAyZlHbkiBJ3MKmPPWgrErUAC3O1P7Fx7
ibzUQxRESVUUA6e+5ggld33iH4SaPHFZPGSziOxUIETenmLhfHHgXbWRgMiS0hAU
wo1a/QljqLezprXdhH38sVGMtjymshrKiN+jEdhwScagdMiWiFCm9caJntGEcTV4
tBIEqQZMhGWCgjOh+0wfqBI591K3ir7ymnU7+R3TEcPw1yGIQAHzcJLA0WQ8fFoM
Iz5i0/WiFODwG++MepVf/Gx8er+EoZYtp/s8PRfDmxIJF0Ndj/TsI0bfoGl2CmRz
bXVaUGaAurOvyukMhxpgReewJE2TsDpIOxexRemsGBPjAgMBAAE=
-----END PUBLIC KEY-----
RSA Private-Key: (3072 bit, 2 primes)
modulus:
00:ca:ef:5c:d7:dd:be:a9:b0:20:e1:de:35:7e:08:
90:23:a1:d0:dc:05:6c:4c:8e:a4:06:e7:dc:b6:7d:
b6:58:78:d2:fd:69:6b:3a:0a:91:d7:91:dc:29:fd:
94:19:e5:a3:8e:80:57:fa:9c:7a:6d:a9:ff:55:96:
5b:0f:e1:0e:10:39:60:a0:b3:fd:ce:96:b2:ef:29:
90:23:cb:2c:76:a8:db:00:15:52:d9:10:c2:d4:b6:
60:f9:c4:81:d5:dd:0f:5f:1f:1b:7e:79:b7:2d:ca:
24:72:c5:0f:44:61:69:a0:70:8f:79:18:56:12:90:
6d:fa:b6:07:37:70:84:84:21:73:ad:c2:14:21:aa:
cf:03:26:65:1d:b9:22:04:9d:cc:2a:63:cf:5a:0a:
c4:ad:40:02:dc:ed:4f:ec:5c:7b:89:bc:d4:43:14:
44:49:55:14:03:a7:be:e6:08:25:77:7d:e2:1f:84:
9a:3c:71:59:3c:64:b3:88:ec:54:20:44:de:9e:62:
e1:7c:71:e0:5d:b5:91:80:c8:92:d2:10:14:c2:8d:
5a:fd:09:63:a8:b7:b3:a6:b5:dd:84:7d:fc:b1:51:
8c:b6:3c:a6:b2:1a:ca:88:df:a3:11:d8:70:49:c6:
a0:74:c8:96:88:50:a6:f5:c6:89:9e:d1:84:71:35:
78:b4:12:04:a9:06:4c:84:65:82:82:33:a1:fb:4c:
1f:a8:12:39:f7:52:b7:8a:be:f2:9a:75:3b:f9:1d:
d3:11:c3:f0:d7:21:88:40:01:f3:70:92:c0:d1:64:
3c:7c:5a:0c:23:3e:62:d3:f5:a2:14:e0:f0:1b:ef:
8c:7a:95:5f:fc:6c:7c:7a:bf:84:a1:96:2d:a7:fb:
3c:3d:17:c3:9b:12:09:17:43:5d:8f:f4:ec:23:46:
df:a0:69:76:0a:64:73:6d:75:5a:50:66:80:ba:b3:
af:ca:e9:0c:87:1a:60:45:e7:b0:24:4d:93:b0:3a:
48:3b:17:b1:45:e9:ac:18:13:e3
publicExponent: 65537 (0x10001)

privateExponent:
43:d2:91:b5:f7:7f:34:59:0f:f4:4c:fe:95:bb:a8:
e8:af:b9:0c:ff:a6:fd:43:22:e0:c7:f7:04:ea:a8:
d9:92:af:f9:4f:95:2d:95:c0:be:4a:1a:49:d2:5c:
ff:f6:b6:9d:f6:98:f0:c2:01:4c:cb:66:f1:a4:c9:
94:5a:04:08:3a:14:e8:40:9f:8f:be:df:d8:7c:8c:
96:d9:dd:67:5e:f1:aa:6a:76:00:e3:d0:29:a5:36:
6d:e3:55:fd:32:df:63:4c:13:35:46:da:88:ac:29:
58:4e:31:d7:09:b3:72:92:8b:f0:cd:c8:5e:75:f4:
bb:b8:c0:5a:af:f9:29:eb:c0:2c:8f:53:89:18:fc:
0c:b2:75:52:e4:bf:d0:c9:28:25:f6:ab:a3:0d:3c:
44:26:c3:8e:30:a5:e8:79:d4:33:e9:6f:0b:68:27:
96:56:9f:d4:c4:e8:51:1a:e1:e2:b8:a8:ad:1d:f5:
2a:44:3b:ad:aa:7e:32:41:c1:af:f3:33:d6:dc:c4:
b5:3c:32:64:51:c0:19:34:7b:cd:37:7b:73:8d:7a:
16:ab:51:81:3d:3f:e4:16:e6:36:2b:df:4b:a4:72:
c8:c9:b3:72:4e:87:94:4e:8c:ea:4b:d0:25:5c:e2:
c5:8e:00:bf:70:54:76:f8:21:24:bb:19:af:b0:7f:
1b:10:a9:c8:cf:83:38:12:3c:79:0f:40:9d:10:5b:
db:8a:bf:9a:70:fb:d0:46:7e:72:75:8e:08:e5:e5:
fd:39:b0:34:a2:e1:a5:29:6f:00:22:45:8d:c6:22:
6e:bb:20:e7:0a:05:87:da:9c:a2:ce:75:47:b4:4b:
c4:af:45:68:d5:e7:31:c1:8b:4e:87:f4:f4:a6:fe:
0e:cb:ec:37:a3:50:4b:2e:64:90:5a:03:a5:b4:b9:
5e:61:ce:8d:1b:5f:63:7f:a0:cb:ab:0a:df:42:9f:
18:60:1b:52:c3:b3:01:fc:c6:70:72:a3:8a:d8:4f:
c2:c4:00:21:ac:49:b6:60:99
prime1:
00:f7:a3:94:86:0d:33:8f:6b:81:eb:7f:38:69:c7:
09:b7:cd:f6:73:29:43:65:3b:09:03:f5:f8:0e:bb:
82:f5:4f:d5:b6:65:3c:e1:f1:5a:e9:6b:2a:aa:99:
96:60:dd:fe:10:95:41:ee:10:07:20:87:7a:22:85:
af:d6:ff:de:b2:e7:24:d9:8e:50:f0:a1:5d:74:b4:
8c:62:4c:d2:59:24:07:ad:ba:03:cd:a7:63:2c:83:
c6:24:40:4f:bb:1a:cd:4d:03:3a:a9:d9:9f:2f:14:
63:21:87:62:85:23:36:e7:e9:ff:6c:f0:fd:5a:84:
05:9c:7c:7f:b1:19:3d:20:15:b8:33:27:92:5d:1c:
4c:88:1c:53:4d:1c:f5:a8:b1:fa:c2:77:53:9b:30:
fc:f8:ed:87:76:2e:35:b7:ad:58:67:bf:bd:9c:a9:
db:91:7a:15:5b:75:2e:48:30:4d:67:1d:ea:10:c9:
51:75:09:37:5d:2f:b9:e8:92:32:9d:29:6d
prime2:
00:d1:c9:64:6e:85:c7:8d:aa:4e:4a:0b:74:37:bd:
ff:00:c7:58:3d:bf:59:e3:df:04:c7:d0:7a:59:ee:
07:e6:63:d7:68:3b:69:88:54:0d:2a:7b:21:3c:9c:
7a:4f:fb:e1:fa:e8:29:7e:0f:71:5b:c1:61:14:93:
31:20:50:6d:7d:90:80:95:66:55:6a:4d:cc:65:85:
6c:4b:75:c8:79:fe:46:fc:0a:5a:2b:d7:cb:5a:96:
88:cb:b0:e9:d1:09:68:30:c0:6f:2d:53:ef:4d:03:
c3:79:f0:3a:40:8c:97:60:a0:69:51:64:d4:41:fc:
fb:11:c3:72:0a:1e:56:f6:ce:f0:fa:68:e3:e0:f9:
54:89:0c:fc:ab:47:4a:37:b6:9b:0c:38:06:be:b3:
bc:1d:af:c9:86:4e:80:83:98:4d:5a:15:8a:fd:d1:
11:bc:f1:4c:3b:4f:7f:ba:2c:b5:85:cf:8d:e3:d1:
42:39:be:7b:7b:a0:19:3d:6d:c8:3f:b0:8f
exponent1:
00:c0:6c:0f:40:8a:89:81:eb:db:ac:0d:d2:db:fe:

```
99:02:85:bb:f6:88:1d:a2:4f:59:16:06:ce:95:44:
06:e2:6f:02:75:13:fd:56:e3:9f:ec:b8:25:13:22:
fc:c2:90:3c:96:ce:23:c8:c4:13:85:a7:3f:b4:0b:
85:32:de:e7:40:c4:72:d1:c9:d0:02:ea:a0:1f:cb:
1b:3a:56:cf:2c:0c:df:1a:92:eb:d9:a5:33:5e:a7:
96:13:1d:15:d7:21:60:5d:73:20:e6:51:ff:6b:29:
c0:4d:91:51:70:7a:88:73:74:53:d1:67:00:b6:90:
d7:7b:5d:12:2b:9e:9c:ec:8d:73:ef:eb:d3:c3:1d:
f6:29:dd:38:ad:36:cf:7c:21:af:e3:e3:ac:c7:6e:
2d:63:8f:ce:2e:7a:81:ab:13:bb:1a:02:d7:67:20:
65:48:89:40:87:2c:6a:a6:15:42:4f:d9:e2:c2:e0:
6b:b7:31:4e:1f:ce:b1:fa:91:7f:5a:b7:91
exponent2:
66:4a:e1:21:d3:31:9e:ae:30:46:82:97:44:a6:ec:
34:a0:ff:31:fc:a0:04:30:b6:d0:07:a3:e1:3d:e3:
b4:3f:72:c5:6c:52:e5:1a:b6:e0:c3:f1:4c:f0:af:
e3:58:5a:b4:51:88:09:e3:d5:ce:7b:d8:ae:83:a7:
2c:ae:8a:f4:f3:04:ff:d4:4a:49:ef:6d:7f:03:33:
ef:07:9b:9d:80:93:74:4a:47:f5:a0:df:93:68:5b:
83:96:dc:2c:05:7e:3c:67:58:ce:ad:62:be:16:db:
b6:15:a1:11:e0:7b:df:ad:d8:2c:cc:11:83:ab:ab:
70:d9:f0:3d:66:d5:d8:ba:c7:5e:12:cf:2a:df:e8:
8c:7b:3c:a8:f7:b6:04:bc:91:95:bf:ab:ea:49:11:
ad:18:0e:17:e3:27:5f:03:60:94:50:74:d9:96:9c:
23:99:35:26:a6:79:0d:7a:c7:78:5b:e0:3f:f9:c5:
65:0a:b0:83:73:69:5b:3e:b0:a9:fd:99
coefficient:
00:a9:4d:7c:f7:f0:55:1a:b8:16:9c:97:ef:46:5b:
fc:0f:61:bf:25:d7:e8:07:85:8d:a1:5e:e3:6a:fa:
2b:8b:56:ca:c9:a1:62:7c:fd:7e:ba:71:79:3b:3c:
52:df:40:70:26:c5:09:ef:2e:e6:c6:ec:b4:6e:77:
1e:6a:85:74:d8:de:b2:da:38:f2:b2:2c:45:03:f7:
b4:70:fb:42:f8:42:7c:f9:be:62:58:5f:28:74:f8:
cc:23:5f:dd:1a:52:23:43:d9:64:be:34:07:11:d3:
30:bf:ad:bb:5b:a4:1e:a4:0c:d0:9d:35:a7:b8:e8:
8c:39:7d:27:76:f0:cc:eb:80:43:0b:2a:9e:80:cd:
07:22:c0:8a:49:69:ea:56:80:c9:ed:58:09:86:36:
44:4e:56:36:19:78:5b:57:7f:d3:b5:c2:9e:04:96:
9d:34:8e:fb:9c:5a:05:3f:21:d4:fc:56:01:7d:6f:
6b:2e:12:8c:e7:85:04:af:7a:83:0f:60:3b
```

Refer below example of the **non-readable key** in the Linux server.

```
root@linux_server:~# openssl pkey -in .ssh/id_dsa -pubout -text

unable to load key
139734109644096:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting:
ANY PRIVATE KEY
```