

# Experiment 12

## USE OF SECURE SOCKET LAYER

### 12.1 Aim

To familiarize the use of Secure Socket layer.

### 12.2 Theory

Secure Sockets Layer is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

Working:

- In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.
- The secret key is encrypted by using a receiver's public key.

SSL can only be implemented by websites that have an SSL certificate (technically a "TLS certificate"). An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

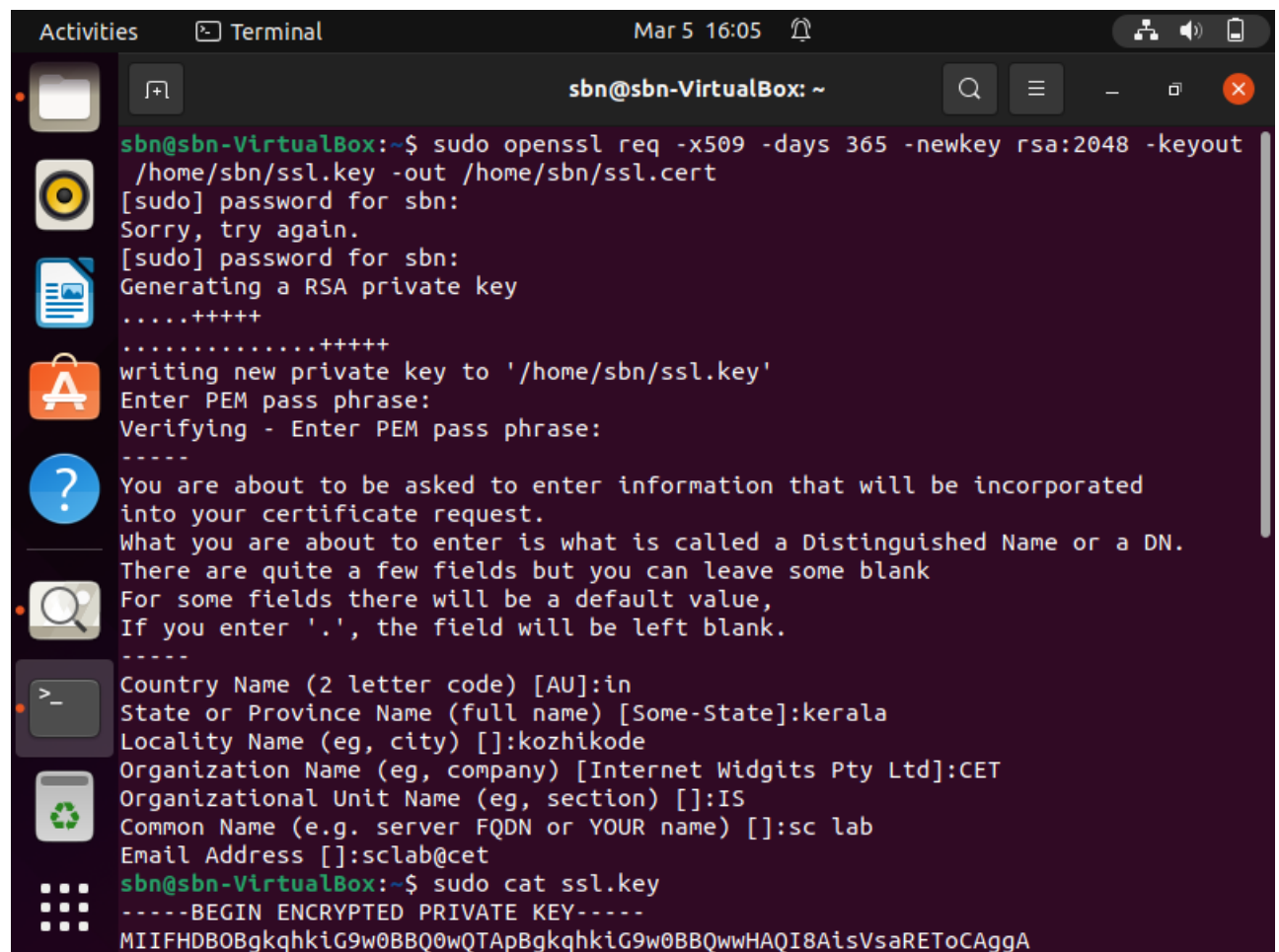
There are several different types of SSL certificates.

- Single-domain: A single-domain SSL certificate applies to only one domain.
- Wildcard: Like a single-domain certificate, a wildcard SSL certificate applies to only one domain. However, it also includes that domain's sub-domains.
- Multi-domain: As the name indicates, multi-domain SSL certificates can apply to multiple unrelated domains.

SSL certificates also come with different validation levels. A validation level is like a background check, and the level changes depending on the thoroughness of the check.

- Domain Validation: This is the least-stringent level of validation, and the cheapest. All a business has to do is prove they control the domain.
- Organization Validation: This is a more hands-on process: The CA directly contacts the person or business requesting the certificate. These certificates are more trustworthy for users.
- Extended Validation: This requires a full background check of an organization before the SSL certificate can be issued.

## 12.3 Output

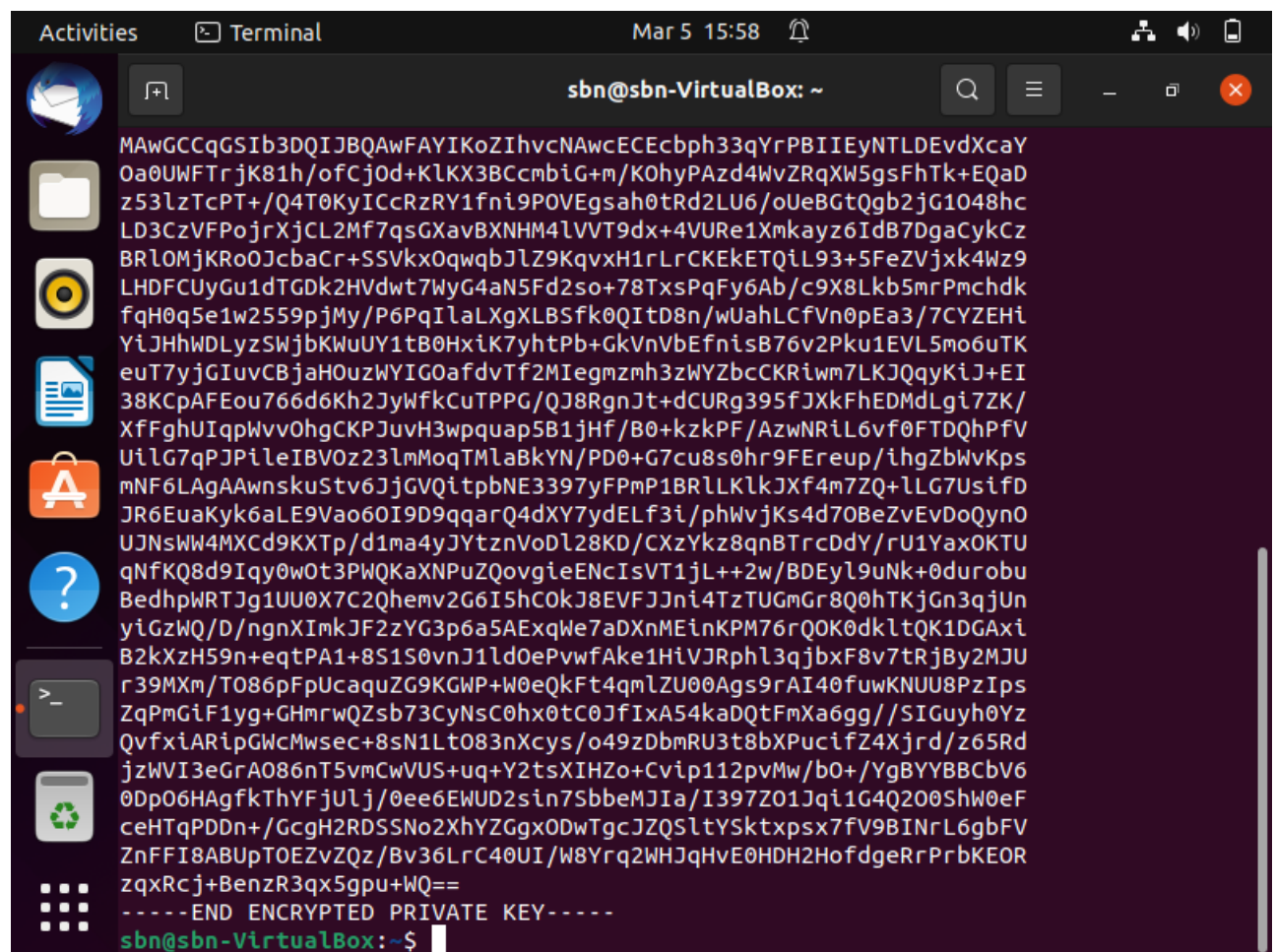


```

sbn@sbn-VirtualBox:~$ sudo openssl req -x509 -days 365 -newkey rsa:2048 -keyout
/home/sbn/ssl.key -out /home/sbn/ssl.cert
[sudo] password for sbn:
Sorry, try again.
[sudo] password for sbn:
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/home/sbn/ssl.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:in
State or Province Name (full name) [Some-State]:kerala
Locality Name (eg, city) []:kozhikode
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CET
Organizational Unit Name (eg, section) []:IS
Common Name (e.g. server FQDN or YOUR name) []:sc lab
Email Address []:sclab@cet
sbn@sbn-VirtualBox:~$ sudo cat ssl.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI8AisVsAREToCaggA

```

Figure 1: Using SSL



The image shows a terminal window titled "sbn@sbn-VirtualBox: ~". The terminal displays a long, multi-line string of alphanumeric characters, which is an encrypted private key. The string is preceded by a series of dashes and the text "END ENCRYPTED PRIVATE KEY". The terminal prompt "sbn@sbn-VirtualBox:~\$" is visible at the bottom.

```
MAWGCCqGSib3DQIJBQAwFAYIKoZIhvcNAwECEcbph33qYrPBIIeYNTLDEvdXcaY
0a0UWFTrjK81h/ofCjOd+KLKX3BccmbiG+m/K0hyPAzd4WvZRqXW5gsFhTk+EQaD
z53LzTcPT+/Q4T0KyICcRzRY1fni9P0VEgsah0tRd2LU6/oUeBGtQgb2jG1048hc
LD3CzVFpOjrXjCL2Mf7qsGXavBXNHM4LVVT9dx+4VURe1Xmkayz6IdB7DgaCykCz
BRlOMjKR0OJcBaCr+SSVx0qwqbJLZ9KqvXh1rLrCKEKETQiL93+5FeZVjxk4Wz9
LHDFCUyGu1dTGdK2HVdwt7WYG4aN5Fd2so+78TxsPqFy6Ab/c9X8Lkb5mrPmchdk
fQh0q5e1w2559pjMy/P6PqILaLXgXLBSfk0QItD8n/wUahLCfVn0pEa3/7CYZEHl
YiJHhWDLyzSWjbKWuUY1tB0Hxik7yhtPb+GkVnVbEfnisB76v2Pku1EVL5mo6uTK
euT7yJGIuvCBjaH0uzWYIG0afdvTf2MIegmzmh3zWYZbcCKRiwm7LKJQyKiJ+EI
38KCpAFEou766d6Kh2JyWfKCuTPPG/QJ8RgnJt+dCURg395fJXkFhEDMdLgi7ZK/
XfFghUIqpWvv0hgCKPJuvH3wpquap5B1jHf/B0+kzkPF/AzwNRiL6vf0FTDQhPfv
UilG7qPJpIleIBVOz23lmMoqTmlaBkYN/PD0+G7cu8s0hr9FEreup/ihgZbWvKps
mNF6LAGAAwnskuStv6JjGVQitpbNE3397yFPMp1BRlLKlkjXf4m7ZQ+llG7UsifD
JR6EuaKyk6aLE9Vao60I9D9qqarQ4dXY7ydeLf3i/phWvjKs4d70BeZvEvDoQyn0
UJNSWW4MXCd9KXTP/d1ma4yJYtznVoDl28KD/CXzYkz8qnBTrcDdY/rU1Yax0KTU
qNfKQ8d9Iqy0wOt3PWQKaXNPuZQovgieENCIsVT1jL++2w/BDEyl9uNk+0durobu
BedhpWRTJg1UU0X7C2Qhemv2G6I5hCokJ8EVFJJni4TzTUGmGr8Q0hTKjGn3qjUn
yiGzWQ/D/ngnXImkJF2zYG3p6a5AExqWe7aDXnMEinKPM76rQ0K0dkltQK1DGAXi
B2kxZH59n+eqtPA1+8S1S0vnJ1ld0ePvwfAke1HiVJRphl3qjbxF8v7tRjBy2MJU
r39MXm/T086pFpUcaquZG9KGWP+W0eQkft4qmlZU00Ags9rAI40fuwKNUU8PzIps
ZqPmGiF1yg+GHmrwQZsb73CyNsC0hx0tC0JfIXA54kaDQtFmXa6gg//SIGuyh0Yz
QvfxiARipGwCmwsec+8sN1Lt083nXcys/o49zDbmRU3t8bXPucifZ4Xjrd/z65Rd
jzWVI3eGrA086nT5vmCwVUS+uq+Y2tsXIHZo+Cvip112pvMw/b0+/YgBYBBcbV6
0Dp06HAGfkThYfjUlJ/0ee6EWUD2sin7SbbeMJia/I397Z01Jqi1G4Q200ShW0eF
ceHTqPDDn+/GcgH2RDSSNo2XhYZGgX0DwTgcJZQSltySktxpsx7fv9BINrL6gbFV
ZnFFI8ABUpTOEZvZQz/Bv36LrC40UI/W8Yrq2WHJqHvE0HDH2HofdgeRrPrbKEOR
zqxRcj+BenzR3qx5gpu+WQ==
-----END ENCRYPTED PRIVATE KEY-----
sbn@sbn-VirtualBox:~$
```

Figure 2: Encrypted private key

## 12.4 Result

Successfully familiarized the use of Secure Socket layer .