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

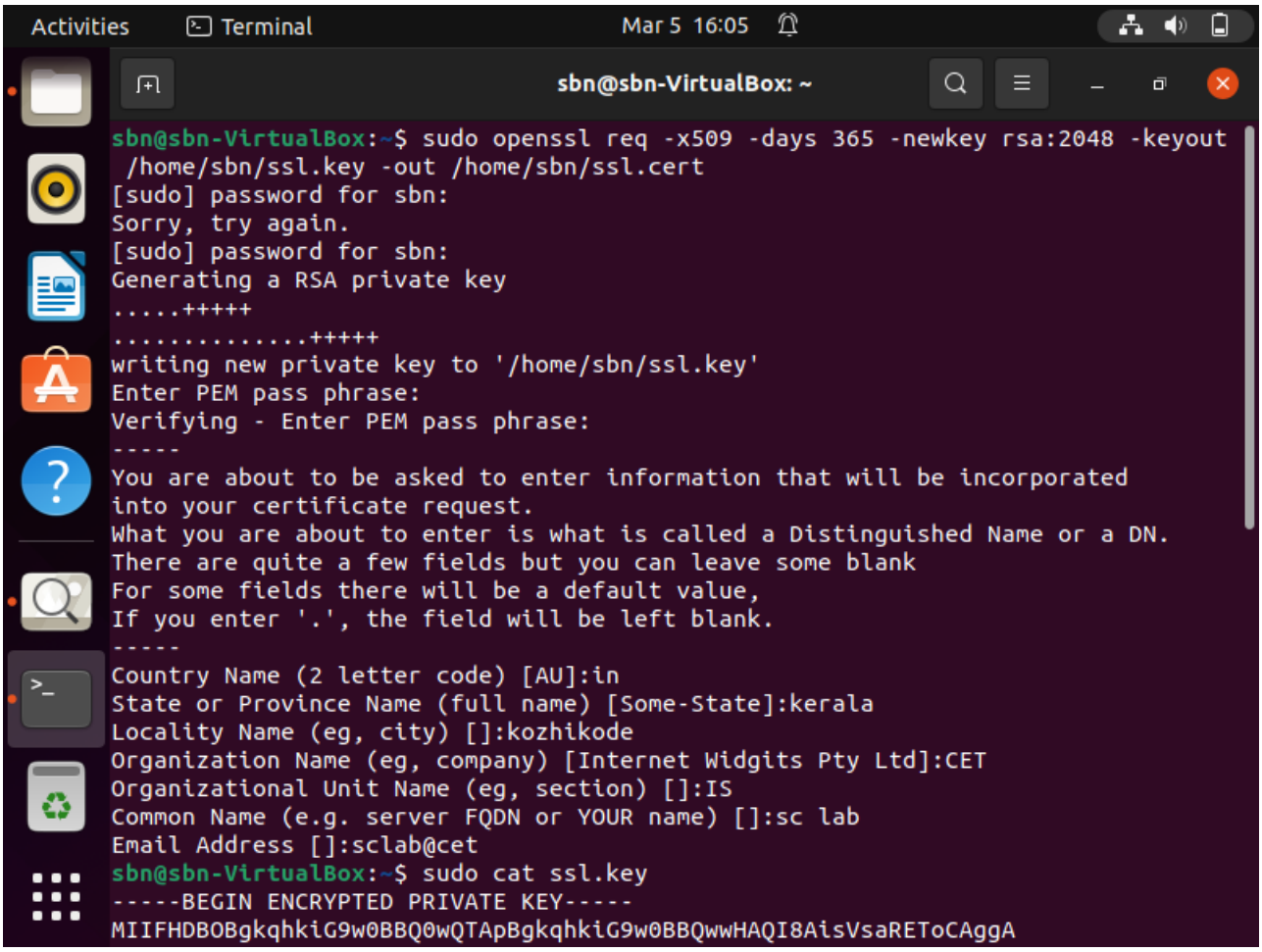

Figure 1: Using SSL

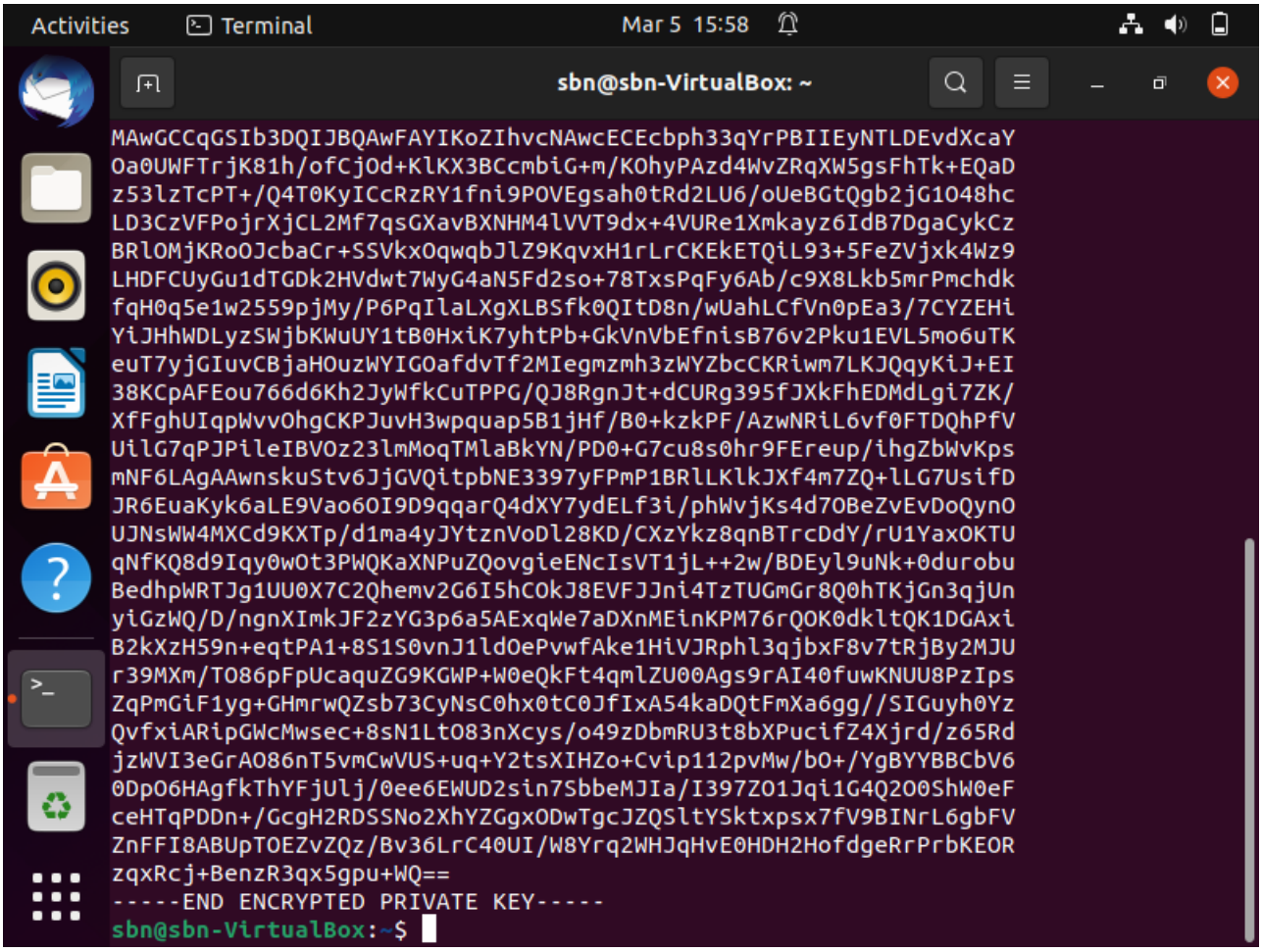

Figure 2: Encrypted private key

12.4 Result

Successfully familiarized the use of Secure Socket layer .