What is SSL & how to

Create an SSL certificate in Linux

Read more >

Aswin KS

What is SSL

Secure Sockets Layer (SSL) is a protocol for securing communication on the Internet.

It helps to encrypt data sent between source and destination, preventing third parties from reading it while it’s in transit.

Aswin KS

What is HTTPS

HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate.

HTTPS in the URL indicates that data transfer between the source and destination device is encrypted using an SSL certificate.

Aswin KS

How SSL encrypt traffic?

How SSL encrypt traffic

SSL uses 2 types of encryption

1. Asymmetric encryption

- It uses a key pair to encrypt and decrypt data. one key is shared with anyone interested in communication. This is called Public Key. The other key in the key pair is kept secret and is called Private Key

- Examples of asymmetric key encryption algorithms are RSA, DSA

How SSL encrypt traffic

2. Symmetric encryption

• It uses only one key which encrypts and decrypts the data. Both sender and receiver should have this key, which is only known to them.

Asymmetric encryption is used to establish a secure session between a client and a server, and symmetric encryption is used to exchange data within the secured session.

• Example: AES-128, AES-192, and AES-256.

Types of SSL certificates

Types of SSL Certificates

1. CA-signed Certificates: These SSL certificates are signed by well-trusted organizations. They are trusted by most browsers.

2. Self-Signed Certificates: A self-signed SSL certificate is created and authorized by an individual. The only downside is most browsers will not trust the certificate and may show a warning message to the user.

Aswin KS

Create Self-signed SSL Certificate

Create SSL Certificate

We will use the OpenSSL utility to create an SSL certificate

Command to generate a certificate

```
openssl req -newkey rsa:4096 \
        -x509 \
        -sha256 \
        -days 3650 \
        -nodes \
        -out mycertificate.crt \
        -keyout mycertificate.key
```

Explanation of Command

-newkey rsa:4096 - Creates a new certificate request and 4096 bit RSA key.

-x509 - Creates a X.509 Certificate.

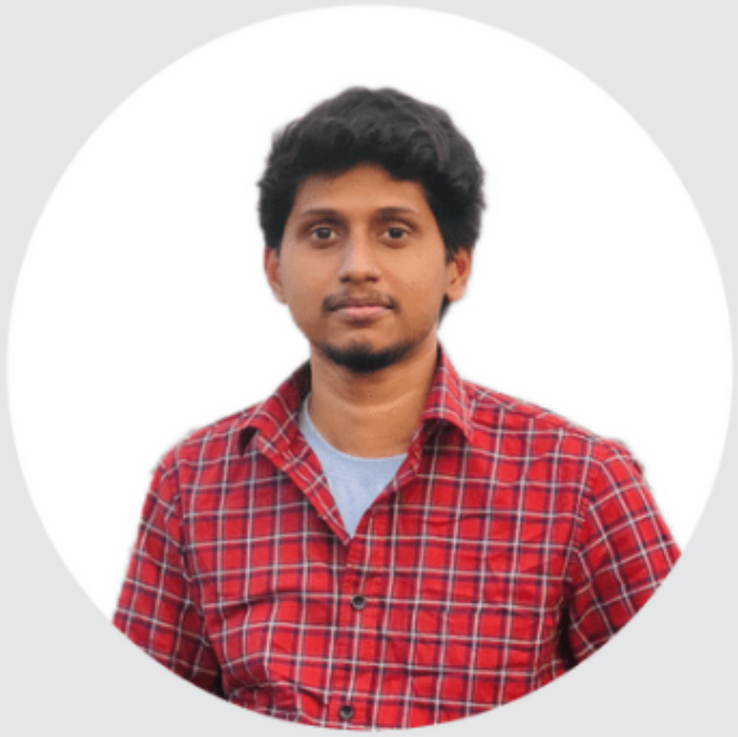
-sha256 - Use 265-bit SHA (Secure Hash Algorithm).

-days 3650 - The number of days the certificate is valid for.

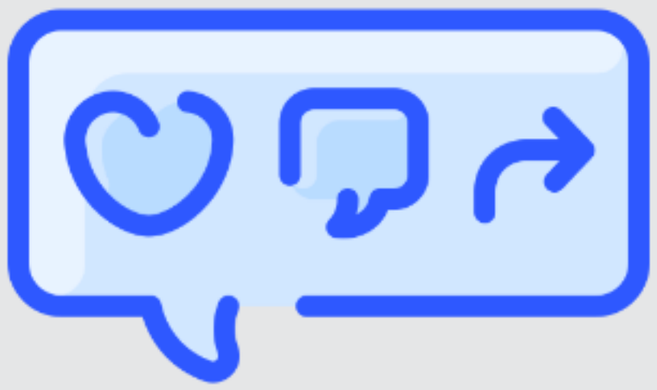
-nodes - Creates a key without a passphrase.

-out mycertificate.crt - Specifies the filename for newly created certificate.

-keyout mycertificate.key - Specifies the filename to write the newly created private key.



Aswin KS



www.linkedin.com/in/aswinks-profile