



HOME > LINUX

How to Create a Self-Signed Certificate in Linux

Generating a self-signed certificate is rather easy on Linux. Here's how you can create one from the Linux terminal.

BY JT MCGINTY
PUBLISHED NOV 11, 2021



Creating a self-signed SSL certificate in Linux is quite easy and can be done in just a few clicks. You can use a self-signed certificate to secure the connection between your web server and a visitor's browser. Linux makes it really easy for you to generate a certificate and sign it using a private key.

Here's how you can create your own SSL certificates right from your Linux terminal.

What Is an SSL Certificate?

SSL stands for Secure Socket Layer. [An SSL certificate](#) verifies the identity of a website and enables an encrypted (secure) connection between the website and your browser.

A secure connection will encrypt all data sent back and forth between your web browser and the server you are communicating with. This prevents any person or [computer in the middle from intercepting](#) and reading the data being transferred.

Can I Use a Self-Signed SSL Certificate on My Website?

You can install and use your own self-signed SSL certificate on your website and to enable encrypted connections. However, since a trusted certificate authority hasn't signed the certificate, visitors' web browsers will show a warning saying so, and state that the site can not be positively identified because of this.

For this reason, self-signed certificates are generally best used for development and testing purposes, or for applications such as a company or home intranet where users are coming from an internal network and not connecting via the internet.

Again, it's important to note that although a self-signed SSL certificate may cause warnings in your web browser, it will still enable a secure connection that works in exactly the same way as any certificate created by one of the trusted authorities.

If you want to generate an SSL certificate for a public website but be sure that users don't receive any confusing warnings, you might want to look into how you can [set up a free](#)

[SSL certificate from a trusted certificate authority.](#)

Installing OpenSSL on Linux

To generate a self-signed SSL certificate on Linux, you'll first need to make sure that you have OpenSSL installed. To do so, open a terminal and enter the appropriate commands corresponding to the distro you're using.

If you are using a Debian-based system such as Ubuntu or Linux Mint:

```
sudo apt install openssl
```

If you are using an RPM-based distro like Fedora or CentOS:

```
sudo dnf install openssl
```

To install OpenSSL on Arch Linux:

```
pacman -S openssl
```

It should take a few moments for your system to download and install the **openssl** package.

Creating Your Self-Signed SSL Certificate

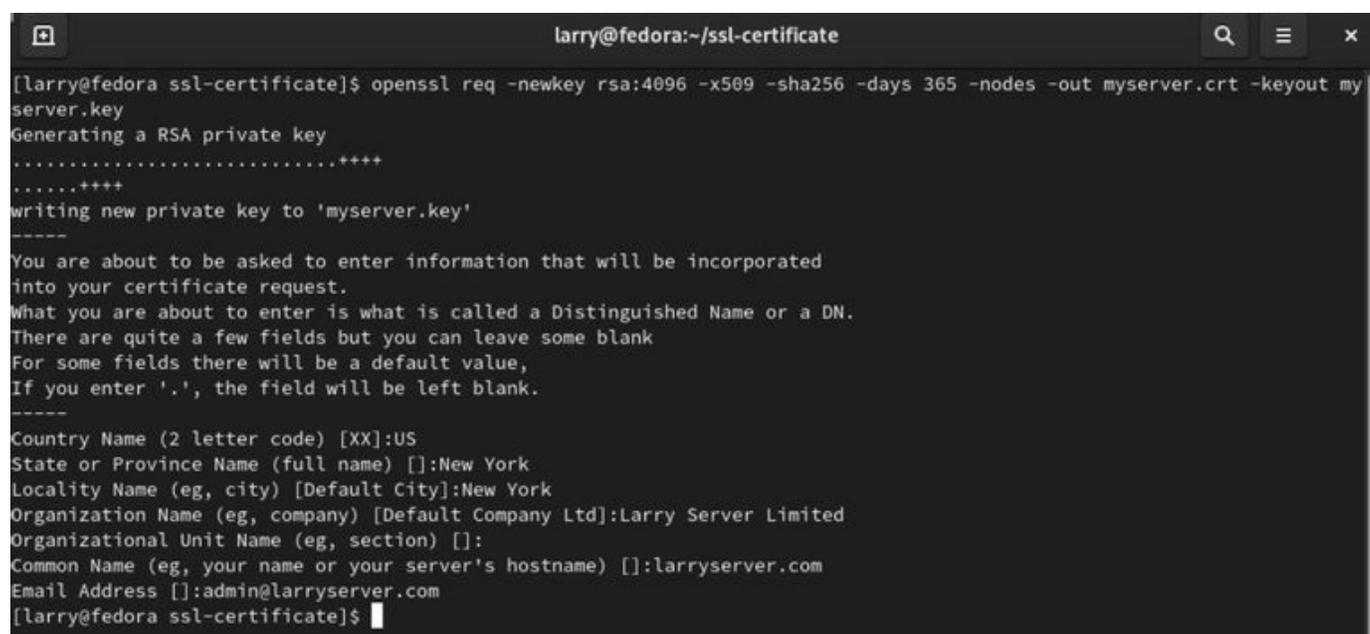
Once you've made sure that you have OpenSSL installed, you can create your SSL certificate by entering a single command. OpenSSL will create the certificate and

corresponding encryption key in the current directory. So, make sure you're in the directory where you want your certificate and key saved before you enter any other commands.

To create your self-signed SSL certificate, enter the following command at the prompt, replacing the two instances of **myserver** with the filenames that you would like to use.

```
openssl req -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out myserver.crt -keyout myserver.key
```

The command will generate a certificate and a private key used to sign the certificate. You can name the files according to your will. The aforementioned command will generate a self-signed certificate using 4096-bit encryption which is valid for 365 days.



```
larry@fedora:~/ssl-certificate
[larry@fedora ssl-certificate]$ openssl req -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out myserver.crt -keyout myserver.key
Generating a RSA private key
.....++++
.....++++
writing new private key to 'myserver.key'
-----
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) [XX]:US
State or Province Name (full name) []:New York
Locality Name (eg, city) [Default City]:New York
Organization Name (eg, company) [Default Company Ltd]:Larry Server Limited
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:larryserver.com
Email Address []:admin@larryserver.com
[larry@fedora ssl-certificate]$
```

To complete the process, the system will ask several questions about the organization the certificate is intended for. If you are just planning to use the certificate for personal development or testing purposes, you can fill in any values you like except for the **Common Name** field. In this field, you should enter the domain name of the website where you plan to install the certificate.

Your SSL Certificate Is Now Ready to Use

That's all there is to it. You should now have an SSL certificate (CRT file) and the encryption key (KEY file) used to sign it. Just follow the instructions on the platform where you'd like to install your certificate and you will be able to connect to your website using encrypted HTTPS connections.

Not many Linux users know this but you can also use OpenSSL to encrypt files, entire disk directories, and more.

Encrypt data
on Linux

How to Easily Encrypt and Decrypt Files and Directories in Linux

READ NEXT >



RELATED TOPICS

LINUX

SECURITY CERTIFICATE

DATA SECURITY

ABOUT THE AUTHOR



JT McGinty

(16 Articles Published)

in

JT is a tech industry veteran with more than 25 years of experience. From tech support to programming and system administration, he has done it all. He particularly enjoys teaching new users the freedom and...

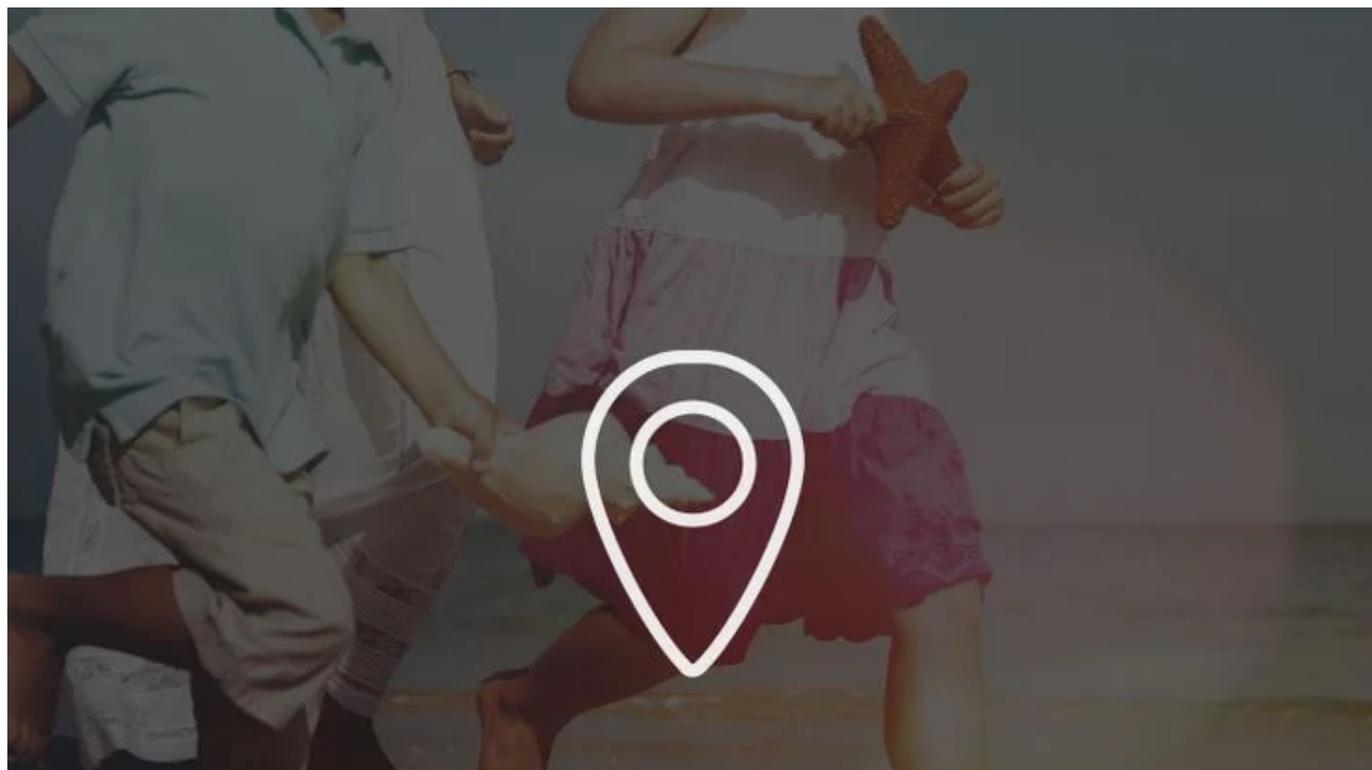
More From JT McGinty →

SUBSCRIBE TO OUR NEWSLETTER

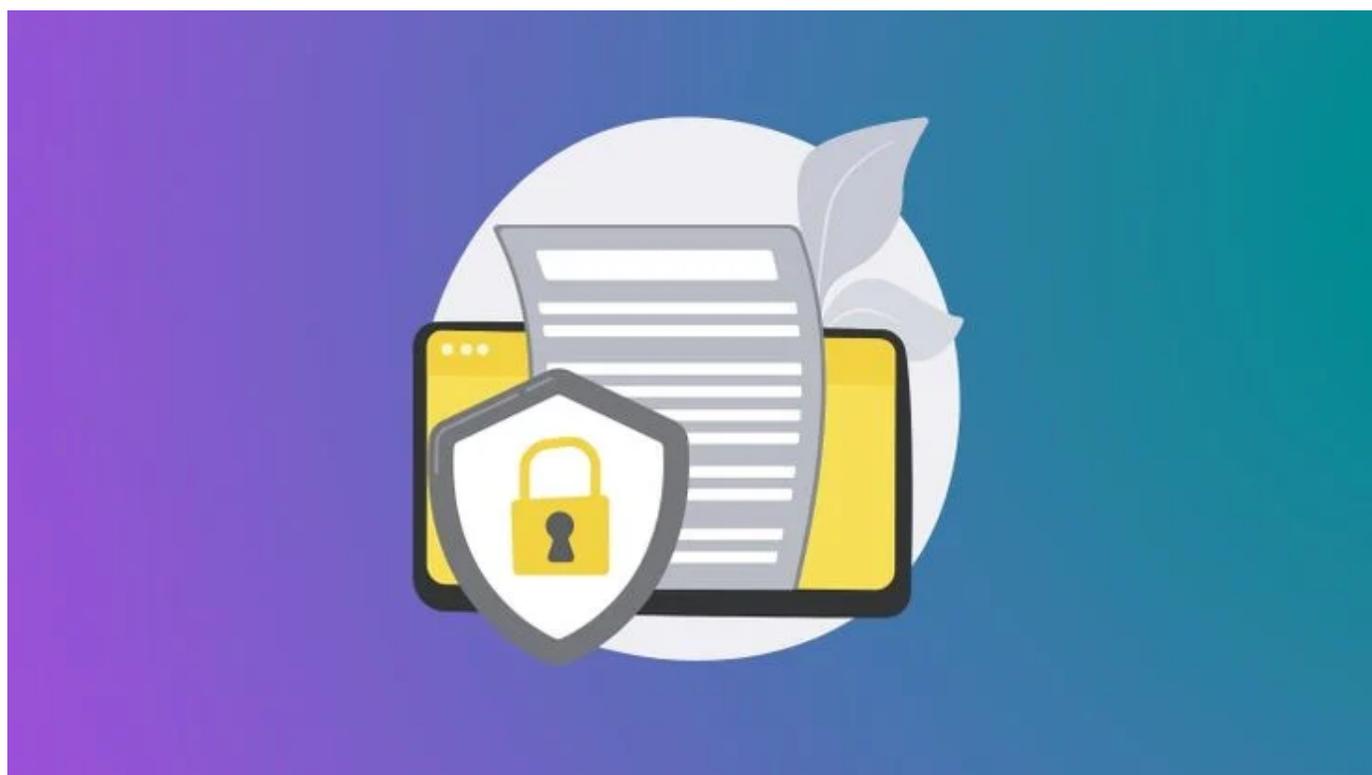
Join our newsletter for tech tips, reviews, free ebooks, and exclusive deals!

CLICK HERE TO SUBSCRIBE

ON THE WIRE



The 7 Best Free Android Apps to Find Your Friends via GPS



How to Spot a Bad Privacy Policy?



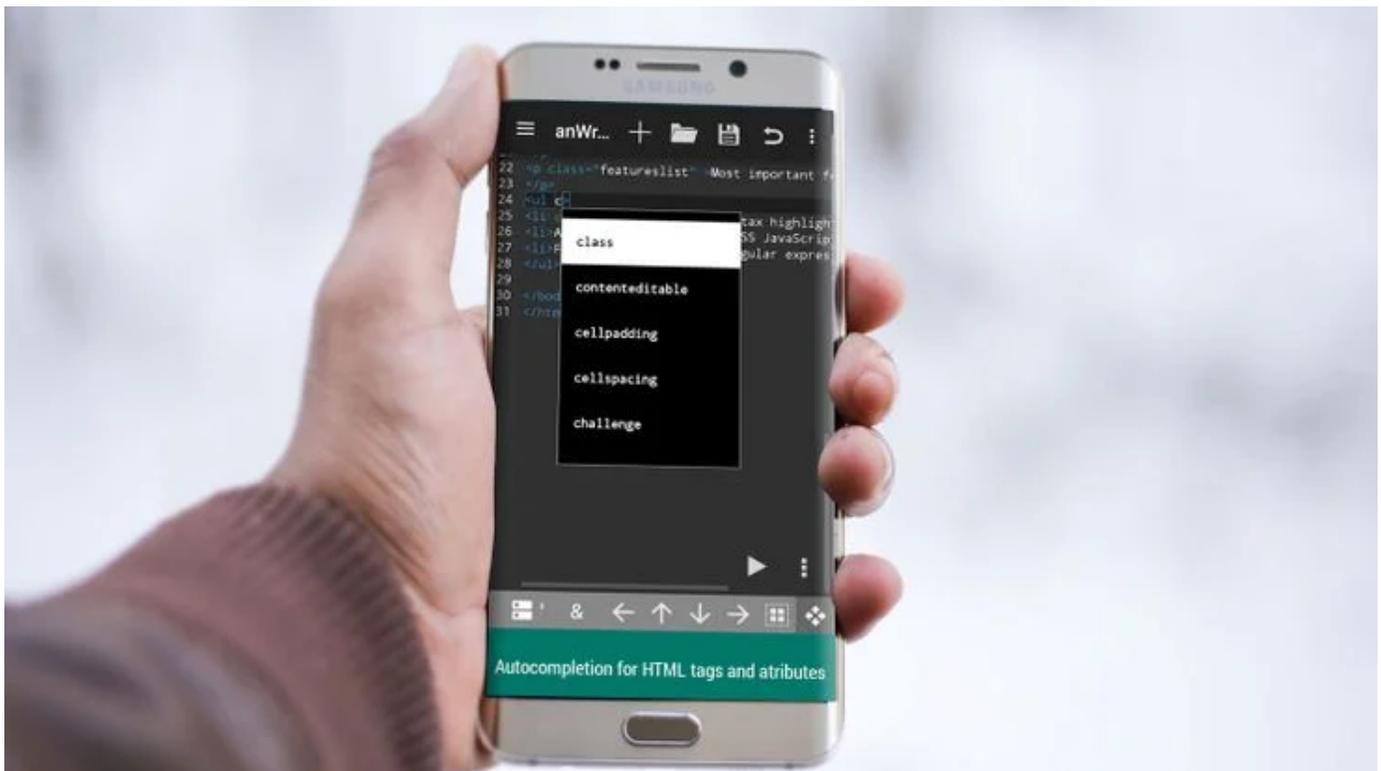
What Is the FreedomPHONE? Is It More Secure Than Android or iPhone?



15 Free Internet TV Channels You Can Watch Online



So You Just Bought an Arduino Starter Kit. What Now?



Yes, You Can Code on the Go: 7 of the Best HTML Editors for Android

READ NEXT

ms-word-templates-business

How to Create Professional Reports and Documents in Microsoft Word

person with laptop

How to Determine Which Streaming Platform Is Worth Your Money

Veiled person behind a PC screen

What Is Browser Isolation? How Can It Help You Against Online Threats?

Airplane flying in the clouds

4 Reasons You Still Cannot Make an In-Flight Call

MacBook sitting beside external hard drive

How to Set Up and Access a Network Drive on a Mac

change user profile folder name windows 11

How to Change the User Profile Folder Name in Windows 11

Commodore PET computer

5 Reasons to Install Linux on an Old Computer

Person playing game on desktop

The 5 Best Game Engines for Beginners in Video Game Development

Photo of a woman smiling at her computer

12 Video Sites That Are Better Than YouTube

[Write For Us](#) [Home](#) [Contact Us](#) [Terms](#) [Privacy](#) [Copyright](#) [About Us](#) [Fact Checking Policy](#)

[Corrections Policy](#) [Ethics Policy](#) [Ownership Policy](#) [Partnership Disclaimer](#)

Copyright © 2022 www.makeuseof.com