matoski.com

Ideas and imagination are boundless

How to generate self-signed certificate for usage in Express4 or Node.js HTTP

written by Ilija Matoski on September 09, 2014– Read in about 4 min · (758 Words) – 6 Comments

node.js openssl ca Certificate Authority Server Certificate generate express ssl certificate self signed certificate

I needed to generate a self-signed certificate for usage with node.js and express, since I don't want to buy a certificate for just trying out and playing with it.

Let's figure out how to do it.

You can also take a look at the following YouTube Video

Make sure you have install **openssl**, if you haven't install it

RHEL/CentOS systems

```
yum install openssl
```

Debian

```
apt-get install openssl
```

To be able to use SSL you need to generate

- Certificate Authority
- Server Certificate

Before we generate anything we need to generate a secure pass phrase

```
# pwgen 50 1 -s > passphrase
# cat passphrase
TNOojiJgDeqP1WwUYflXzBpbfZyl1vkAiuoXoikXRPQ9d1VBkC
```

So that is our secure pass phrase, and whenever it asks you for a pass phrase you can just copy paste the one we generated above.

Let's generate **Certificate Authority** first

Private Key

```
# openssl genrsa -des3 -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
...++++++
...++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
```

Certificate Signing Request

```
openssl req -new -key ca.key -out ca.csr
Enter pass phrase for ca.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) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Signing the certificate

```
# openssl x509 -req -days 365 -in ca.csr -out ca.crt -signkey ca.key
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
Getting Private key
Enter pass phrase for ca.key:
```

Now let's generate the **Server Certificate**

Private Key with pass phrase

```
# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
................................++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

Certificate Signing Request

```
# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.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) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Private Key without pass phrase This will remove the pass phrase from the key, this step is crucial without this it will not work

```
# cp server.key server.key.passphrase
# openssl rsa -in server.key.passphrase -out server.key
openssl rsa -in server.key.passphrase -out server.key
Enter pass phrase for server.key.passphrase:
writing RSA key
```

Signing the certificate

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
Getting Private key
```

These are the files we have now

```
ls -la
total 36
drwxr-xr-x  2 user user 4096 Sep  5 16:19 .
drwxr-xr-x 12 user user 4096 Sep  5 16:09 ..
-rw-r--r--  1 user user  757 Sep  5 16:12 ca.crt
-rw-r--r--  1 user user  603 Sep  5 16:10 ca.csr
-rw-r--r--  1 user user  963 Sep  5 16:09 ca.key
-rw-r--r--  1 user user  757 Sep  5 16:19 server.crt
-rw-r--r--  1 user user  603 Sep  5 16:16 server.csr
-rw-r--r--  1 user user  887 Sep  5 16:18 server.key
-rw-r--r--  1 user user  951 Sep  5 16:17 server.key.passphrase
```

There you go now we have everything needed, lets see how we can create a HTTPS server with node.js

```
var https = require('https'),
    fs = require('fs'),
    express = require('express'),
    app = express();

var secureServer = https.createServer({
    key: fs.readFileSync('./ssl/server.key'),
    cert: fs.readFileSync('./ssl/server.crt'),
    ca: fs.readFileSync('./ssl/ca.crt'),
    requestCert: true,
    rejectUnauthorized: false
}, app).listen('8443', function() {
    console.log("Secure Express server listening on port 8443");
});
```

← Emergency reboot/shutdown using SysRq

Express4 + Mongoose + JSON Web Token Authentication →

6 Comments Warehouse 1 Login

♡ Recommend 1 Share Sort by Best

Join the discussion…

Naresh Kumar • 4 months ago

Thank You so much, It is very helpful

^ | ˅ • Reply • Share ›

David Lewis-Frazier • 5 months ago

This was very helpful. Thank you.

^ | ˅ • Reply • Share ›

Anthony Isaacson • 9 months ago

Great article, thanks so much matoski!

^ | ˅ • Reply • Share ›

Sandesh Magdum • a year ago

This is ridiculously simple article.
Thank you Ilija Matoski :)

^ | ˅ • Reply • Share ›

Christopher Reay • 2 years ago

Absolutely great. Thanks

^ | ˅ • Reply • Share ›

Christopher Reay ➦ Christopher Reay • 2 years ago

Oh, there is one error.

The two times it says:

Please enter the following 'extra' attributesto be sent with your certificate request
A challenge password []:
An optional company name []:

The challenge password should be left blank, unlike what is implied by your text saying "So that is our secure pass phrase, and whenever it asks you for a pass phrase you can just copy paste the one we generated above."

^ | ˅ • Reply • Share ›

ALSO ON **WAREHOUSE**

Automatic starting and stopping of AWS EC2 instances with Lambda and

1 comment • 7 months ago•

amit jayee — Finally found something which on internet which gives precise information about the Cloudwatch event integration with

Automatically switch between WiFi and Ethernet

3 comments • a year ago•

rumassa — Hello!I've changed some words to make it works. I'm using nmcli v0.9.8.8 on Ubuntu 14.04.Instead of "nmcli radio wifi

How to reset folder permissions and ownership to their default in Debian

5 comments • 4 years ago•

Stichoza — Accidentally set /var owner to root:root and even Desktop Environment was not starting properly. Your post helped a lot!

Compile qt 4.8.4 on Ubuntu 10.04 Lucid

1 comment • 4 years ago•

David — Hi, thanks for the easy instructions. I have followed them and did not run into errors in the build process. However, my machine still