



How To Generate SSL Key and Certificate

Version 1.0

TalariaX Pte Ltd

76 Playfair Road
#08-01 LHK2 Building
Singapore 367996

Tel : +65 6280 2881 Fax : +65 6280 6882

Email : info@talariax.com

www.TalariaX.com

REVISION SHEET

Release No.	Date	Description
1.0	13/04/2021	First release

Table of Contents

1.0 Introduction	4
1.1 About TalariaX Pte Ltd	4
1.2 About sendQuick	4
1.3 Purpose of Document	4
2.0 Download and Install XAMPP	5
2.1 What is XAMPP?	5
2.2 XAMPP Control Panel and Shell	5
3.0 OpenSSL Commands	6
3.1 Generate SSL Key	6
3.2 Generate SSL Certificate	8
3.3 Generate CSR	9
3.4 Openssl commands for checking	10

How To Generate SSL Key and Certificate

1.0 Introduction

1.1 About TalariaX Pte Ltd

TalariaX™ develops and offers **enterprise mobile messaging solutions** to facilitate and improve business workflow and communication, and is widely used in areas such as IT alerts & notifications, secure remote access via 2-Factor Authentication, emergency & broadcast messaging, business process automation and system availability monitoring.

In addition to functionality, TalariaX's messaging solutions have also been developed with other key features in mind. These include **security** and **confidentiality** of company information, and **ease in mitigating disruption** during unplanned system downtime such as that arising from cyberattacks.

1.2 About sendQuick

sendQuick is a comprehensive Short Messaging Service (SMS) gateway that is available in the form of an **appliance** or as a **cloud-based** solution. **sendQuick** is used by more than 1,500 businesses, including many Fortune Global 500 companies, in 40 countries and across industries such as banking, finance, insurance, manufacturing, retail, government, education, and healthcare.

1.3 Purpose of Document

This document provides the detailed steps to show how you can generate SSL Key and Certificate that are required when setting up SSL for sendQuick. It includes how you can generate the Certificate Signing Request (CSR) to be submitted to Certificate Authorities (CA) for a CA signed Certificate.

2.0 Download and Install XAMPP

2.1 What is XAMPP?

XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends. We will demonstrate how to generate SSL key, Certificate and CSR using XAMPP.

Download and install XAMPP from the following website:

- <https://www.apachefriends.org/download.html>

2.2 XAMPP Control Panel and Shell

Run XAMPP on your computer and click on **“Shell”**

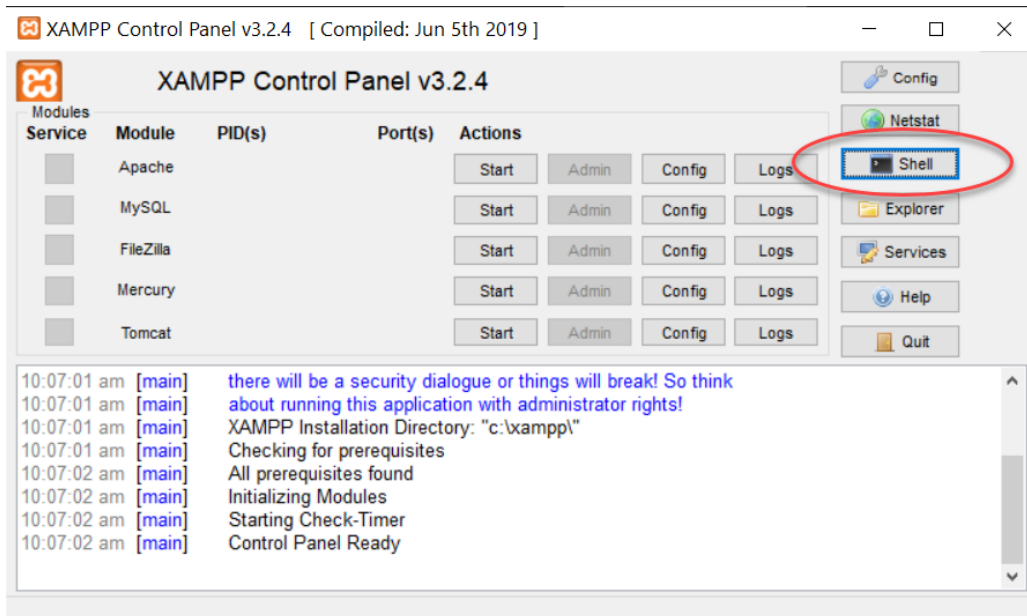


Figure 1: Select “Shell” from XAMPP Control Panel.

The Shell command prompt will appear. Note that the current directory is c:\xampp

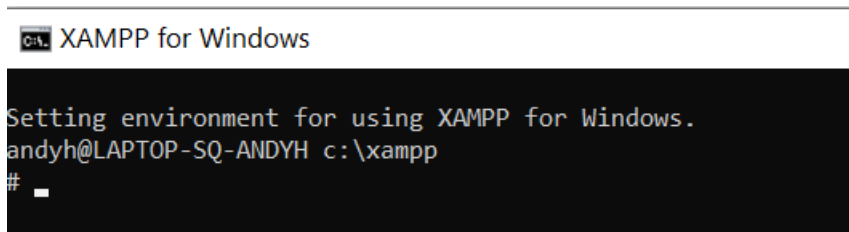


Figure 2: XAMPP Shell Command Prompt.

Before we generate the files, create a subfolder within the xampp folder to make it easier to find the generated files later.

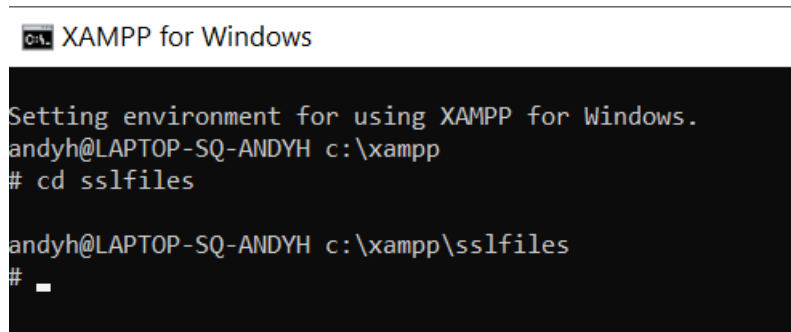
For example, create a new subfolder “sslfiles” i.e. c:\xampp\sslfiles

3.0 OpenSSL Commands

3.1 Generate SSL Key

Step 1: At the shell command, use the following command to change directory to the subfolder we created earlier:

```
# cd sslfiles
```



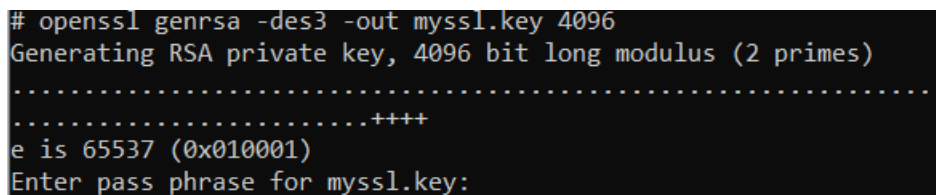
```
Setting environment for using XAMPP for Windows.  
andyh@LAPTOP-SQ-ANDYH c:\xampp  
# cd sslfiles  
andyh@LAPTOP-SQ-ANDYH c:\xampp\sslfiles  
#
```

Figure 3: Change directory to working folder.

Step 2: Generate the SSL key file using the following openssl command. For this example, we will use “myssl.key” as the file name to be generated and using 4096 bits as the size of the private key. You can use any other filenames according to your preference.

For a more detailed understanding of the genrsa command you can refer to openssl manual:

```
# openssl genrsa -des3 -out myssl.key 4096
```

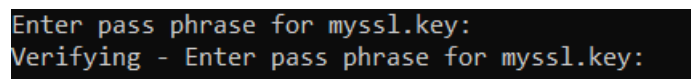


```
# openssl genrsa -des3 -out myssl.key 4096  
Generating RSA private key, 4096 bit long modulus (2 primes)  
.....++++  
e is 65537 (0x010001)  
Enter pass phrase for myssl.key:
```

Figure 4: Generate SSL Key

There will be a prompt to enter a pass phrase for the key file you are generating. For example, we will use “mypass” as the pass phrase. Do remember the pass phrase you have chosen as it will be needed later.

Enter the pass phrase again when asked to verify.



```
Enter pass phrase for myssl.key:  
Verifying - Enter pass phrase for myssl.key:
```

Figure 5: Enter pass phrase for SSL Key file

The SSL Key file is now created. To confirm, you can do a “dir” command at the prompt to see that the file is now available in the directory.

```
andyh@LAPTOP-SQ-ANDYH c:\xampp\sslfiles
# dir
Volume in drive C is Acer
Volume Serial Number is F623-74DC

Directory of c:\xampp\sslfiles

13/04/2021  12:09 pm    <DIR>          .
13/04/2021  12:09 pm    <DIR>          ..
13/04/2021  12:18 pm           3,365 myssl.key
              1 File(s)      3,365 bytes
              2 Dir(s)  183,335,591,936 bytes free
```

Figure 6: SSL Key file generated.

3.2 Generate SSL Certificate

Step 3: Generate the SSL Certificate file using the following openssl command. For this example, we will call the output file “myssl.crt” with 365 days validity. In our example, we use “myssl.key” as our filename for the key file. If you have used your own filename, replace it accordingly in the command.

```
# openssl req -new -x509 -days 365 -key myssl.key -out myssl.crt  
# openssl req -new -x509 -days 365 -key myssl.key -out myssl.crt  
Enter pass phrase for myssl.key:
```

Figure 7: Command to generate SSL Certificate.

Enter the pass phrase that was created earlier for your SSL Key file.

You will then be prompted to answer several questions about your organisation to be incorporated into the certificate.

```
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]:SG  
State or Province Name (full name) [Some-State]:Singapore  
Locality Name (eg, city) []:Singapore  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TalariaX Pte Ltd  
Organizational Unit Name (eg, section) []:Technical Support  
Common Name (e.g. server FQDN or YOUR name) []:sendQuick  
Email Address []:support@talariax.com
```

Figure 8: Information to incorporate into certificate.

The SSL Certificate file is now created. To confirm, you can do a “dir” command at the prompt to see that the file is now available in the directory.

```
# dir  
Volume in drive C is Acer  
Volume Serial Number is F623-74DC  
  
Directory of c:\xampp\sslfiles  
  
13/04/2021 01:41 pm <DIR> .  
13/04/2021 01:41 pm <DIR> ..  
13/04/2021 01:41 pm 4,240 myssl.crt  
13/04/2021 12:18 pm 3,365 myssl.key  
2 File(s) 5,605 bytes  
2 Dir(s) 183,305,654,272 bytes free
```

Figure 9: SSL Certificate file generated.

3.3 Generate CSR

If the requirement is to have the SSL certified by a CA, use the following command to generate the CSR file

```
# openssl req -new -key myssl.key -out myssl.csr
```

You will be prompted for the pass phrase of the ssl key file and to key in information regarding the organisation.

```
# openssl req -new -key myssl.key -out myssl.csr
Enter pass phrase for myssl.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]:SG
State or Province Name (full name) [Some-State]:Singapore
Locality Name (eg, city) []:Singapore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TalariaX Pte Ltd
Organizational Unit Name (eg, section) []:Technical Support
Common Name (e.g. server FQDN or YOUR name) []:sendQuick
Email Address []:support@talariax.com

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

Figure 10: Generate SSL CSR.

The SSL CSR file is now created. To confirm, you can do a “dir” command at the prompt to see that the file is now available in the directory.

```
# dir
Volume in drive C is Acer
Volume Serial Number is F623-74DC

Directory of c:\xampp\sslfiles

13/04/2021  02:04 pm    <DIR>          .
13/04/2021  02:04 pm    <DIR>          ..
13/04/2021  01:41 pm             2,240 myssl.crt
13/04/2021  02:04 pm             1,884 myssl.csr
13/04/2021  12:18 pm             3,365 myssl.key
               3 File(s)              7,489 bytes
               2 Dir(s)  183,302,823,936 bytes free
```

Figure 11: SSL CSR file generated.

3.4 Openssl commands for checking

Following commands to check a certificate and return information of the certificate.

```
# openssl x509 -in myssl.crt -text -noout
```

Check SSL Key and verify consistency

```
# openssl rsa -in myssl.key -check
```

Check SSL CSR

```
# openssl req -text -noout -verify -in myssl.csr
```