



USER MANUAL

MODEL:

**Creating an SSL Certificate
for VIA**

Contents

- Introduction** **2**
- Creating an SSL Certificate** **3**
 - Creating SSL Certificate in Linux 3
 - Creating SSL Certificate in Windows: 4

Introduction

VIA gateway embedded web pages enable you to upload a custom SSL certificate to better provide for the security needs of your organization.

This guide shows you how to create your own SSL certificate.

Creating an SSL Certificate

Create an SSL Certificate in Linux or, if you do not have a Linux base computer available, create the certificate on your Windows computer.

Creating SSL Certificate in Linux



If you do not have OPENSSL installed, use the following command to install it:

```
lars@admin-WStand:~$ sudo apt-get install openssl  
[sudo] password for lars:
```

To create an SSL certificate in Linux:

1. Enter the creation command in the following format:

```
#openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout Server.key  
-out Server.crt
```

The command must include the following elements:

- .key file
- .crt file.
- Required amount of days to be valid.
- At least 2048 bit RSA

2. Press Enter.

3. Fill in the information requested by the system.

```
-----  
Country Name (2 letter code) [AU]:DE  
State or Province Name (full name) [Some-State]:NRW  
Locality Name (eg, city) []:Erkelenz  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kramer Germany  
Organizational Unit Name (eg, section) []:Lars Duziack  
Common Name (e.g. server FQDN or YOUR name) []:Lars  
Email Address []:l.duziack@kramergermany.com
```

4. See your VIA device user manual for instructions to upload the certificate.

Creating SSL Certificate in Windows

If you do not have a Linux base computer available, create the certificate on your Windows computer.



If you do not have the latest stable release of Openssl installed on your computer, download it from the Openssl official website.

To create an SSL certificate in Windows:

1. Open a CMD window as administrator and navigate to your Openssl folder.
2. Navigate to the bin folder and execute the “openssl.exe” file.

```
c:\OpenSSL-Win32>cd bin  
  
c:\OpenSSL-Win32\bin>openssl.exe  
OpenSSL>
```

3. Enter the creation command with the required variables, for example:

```
req -x509 -nodes -days 365 -newkey rsa:4096bits -sha512 -out server.crt -keyout server.key
```
4. If an error message appears, saying that the system is unable to make a certificate request, perform the following steps in an administrator CMD window:
 - a. Set openssl_conf=C:[your path]\bin\openssl.cfg
 - b. Replace the path with your installation path.
 - c. Rerun the certificate variables.
5. Verify that the response is the same as the image below.

```
c:\OpenSSL-Win32\bin>openssl.exe  
OpenSSL> req -x509 -nodes -days 365 -newkey rsa:4096bits -sha512 -out server.crt -keyout server.key  
Generating a 4096 bit RSA private key  
.....++  
.....  
writing new private key to '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]:DE  
State or Province Name (full name) [Some-State]:NRW  
Locality Name (eg, city) []:Heinsberg  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ITSEC  
Organizational Unit Name (eg, section) []:ITSEC  
Common Name (e.g. server FQDN or YOUR name) []:Lars D  
Email Address []:l.duziack@kramergermany.com  
OpenSSL>
```

6. Replace all variables with your own data.

7. Verify that your folder contains the newly created files

```
Verzeichnis von c:\OpenSSL-Win32\bin
23.01.2018 15:52 <DIR> .
23.01.2018 15:52 <DIR> ..
23.01.2018 14:58 <DIR> cnf
23.01.2018 14:58 <DIR> PEM
23.01.2018 15:46 1.024 .rnd
03.11.2017 21:43 6.952 CA.pl
03.11.2017 21:43 45.568 capi.dll
03.11.2017 21:43 27.136 dasync.dll
03.11.2017 21:43 2.093.056 libcrypto-1_1.dll
03.11.2017 21:43 374.784 libssl-1_1.dll
03.11.2017 21:43 970.912 msvcrt120.dll
03.11.2017 21:43 10.771 openssl.cfg
03.11.2017 21:43 429.568 openssl.exe
03.11.2017 21:43 24.064 osslttest.dll
03.11.2017 21:43 34.304 padlock.dll
03.11.2017 21:43 4.826 progs.pl
23.01.2018 15:52 2.152 server.crt
23.01.2018 15:46 3.320 server.key
03.11.2017 21:43 6.779 tsget.pl
```

8. See your VIA device user manual for instructions to upload the certificate.



P/N:



2900-301077

Rev:



1



SAFETY WARNING

Disconnect the unit from the power supply before opening and servicing

For the latest information on our products and a list of Kramer distributors, visit our Web site where updates to this user manual may be found.

We welcome your questions, comments, and feedback.