bbw-it wiki

SSL in Apache

The apache web server which comes as a part of xampp is already configured to use SSL. However, you have to supply it with a valid certificate which must be specific to your serv-er.

Generation of a Server Certificate

In order to run the server with SSL, we need an asymmetric key-pair and a certificate which confirms our ownership of the public key. For this purpose we use the command line tool openssl, which comes as a part of xampp. You find a complete description of openssl under the following link: http://www.openssl.org/docs/apps/openssl.html [http://www.openssl.org/docs/apps/openssl.html] Make sure that you understand exactly what you do in each step and that you understand the purpose of all involved files.

Step 1

First we generate a key pair (public and private key) and a certificate re-quest:

```
openssl req -config openssl.cnf -new -out server_name_version.csr
```

Since we will generate several keys and certificates it is important to keep the naming consistent. As an example you might use *sysw42xx* (xx=your system) as a root name and append a suffix for the versions. The template *server_name_version* in the above example would then be *sysw42xx_v1*.

You are asked by the programme for several pieces of information, whose default values are part of the file *openssl.cnf*. You can either adjust them there or just answer the questions with the correct values. It is up to you which values you enter regarding company, country etc. For the Common Name, however, it is important to enter the value under which you will contact your server (e.g. sysw42xx). When you have answered all the questions, the following two files are created:

privkey.pem
This File contains the private key which you must protect and which must never leave your custody.

server_name_version.csr
A certificate request which contains, among other information, your public key.

Step 2

The public key must now be certified and signed. At first we do this ourselves, thus producing a so called self signed certificate. In order to make live easier we remove first the password on the private key (we will reinsert it later).

```
openssl rsa -in privkey.pem -out server_name_version.key
```

The file server_name_version.key contains now the private key without password protection.

Step 3

Now we create the certificate. This means that we confirm our ownership of the public key by our own digital signature. Of course this is not a very trustworthy action. However, we will use a real certificate agency later on.

```
openssl x509 -in server_name_version.csr -out server_name_version.crt -req -signkey server_name_versi
```

This creates a certificate (.crt) using the certificate request (.csr) and our private key (.key).

Step 4

The two files server_name_version.crt and server_name_version.key are required for the configuration of SSL.

Copy the .crt- and the .key file to the corresponding subdirectory of …./apache/conf (ssl.key und ssl.crt)

Step 5

Adjust the following two entries in the file extra/httpd-ssl.conf:
Variable/Line Set to..
SSLCertificateFile Path to the .crt file
SSLCertificateKeyFile Path to the .key file

Step 6

Stop the web server apache_stop.bat (or button in xampp)

Step 7

restart the web server apache_start.bat (or button in xampp) Test the configuration by calling the server using the ssl-protocol (https).

Step 8

Check the Properties of the certificate in the browser.

Real Certificate

The certificate request which we generated before can now be handed in to a real certificate agency. Usually we would have to deliver some proof of identity and of our ownership of the domain. However, we will use a home made certificate agency run by your teacher who knows you rather well .

1. Copy your certificate request to the folder CSR in your class drive.
2. After your teacher has processed the request you find your certificate in the folder CRT
3. Store this certificate at the appropriate place on your computer.
4. Adjust the configuration in the file httpd-ssl.conf. It must now point to the new cer-tificate.
5. Test the new configuration in the browser.

---

subject/m150/ssl_apache.txt · Last modified: 2016/03/23 17:06 by lp5sduetsch