Apache SSL Zertifikate

Apache: SSL-Konfiguration

Die Konfiguration von SSL ist dann nötig, wenn eine höhere Sicherheit zwischen dem Client und dem Server benötigt wird. In der URL wird dann „https“ anstelle von „http“ geschrieben. HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Web-Server. Er beruht auf X.509-Zertifikaten. Voraussetzung für HTTPS ist der Besitz eines offiziellen Zertifikats für den Web-Server. Dieses erhält man von einer so genannten Zertifizierungsinstanz (Certificate Authority – CA). Die CA garantiert die Echtheit des Servers.

Die für die SSL-Konfiguration wichtigen Dateien befinden sich in der Regel in folgenden Verzeichnissen:

```
xampp\apache\conf\ssl.csr          Zertifikatsdatei       server.csr  /* */
xampp\apache\conf\ssl.key          Schlüsseldatei         server.key  /*enthält private key */
xampp\apache\conf\ssl.crt          Zertifikatsdatei       server.crt  /*Zertifikat mit public key */
```

Zertifikate selber erstellen

Erstellen des „Private Key“

Zunächst ist ein „private Key“ zu generieren. Das SSL-Zertifikat ist nur zusammen mit genau diesem Key gültig. Verliert man den `privat key`, funktioniert auch das Zertifikat nicht mehr. Der `private Key` kann auch nicht aus dem Zertifikat generiert oder sonstwie wiederhergestellt werden. Man sollte also an sicherer Stelle ein Backup des `private keys` aufbewahren.

Man kann den Key auch noch zusätzlich mit einem Passwort schützen, was aber dazu führt, dass man den Webserver nicht ohne Eingabe dieses Passwortes im SSL-Modus starten kann. Aus Sicherheitsgründen wird eine Schlüssellänge von 2048 Bit empfohlen.

Das **openssl-Executable** befindet sich in der Regel in folgendem Verzeichnis:

```
xampp\apache\bin
```

Folgender Befehl muss eingegeben werden:

```
J:\xampp\apache\bin>openssl genrsa –out server.key 2048
```

Certificate Signing Request (CSR) anlegen

Die CSR enthält die Firmeninformationen, Domainname, Email-Adresse usw. Diese Datei sendet man dann an die Zertifizierungsstelle und erhält das Zertifikat zurück.

Alternativ kann man sich aus dem CSR auch ein selfsigned certificate erstellen.

Folgender Befehl muss eingegeben werden:

```
J:\xampp\apache\bin>openssl req -config openssl.cnf -new -key server.key -out server.csr
```

CSR überprüfen

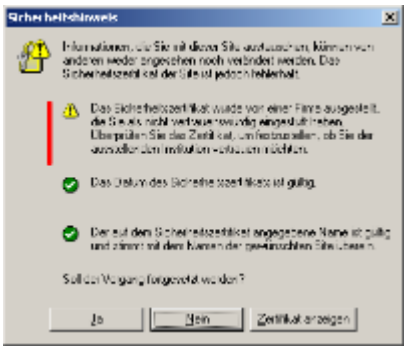
Mit folgendem Befehl kann festgestellt werden, ob alle Angaben im CSR korrekt sind:

```
J:\xampp\apache\bin>openssl req -noout -text -in server.csr
```

Self-signed Certifcate erstellen

Für Testzwecke kann man sich auch das SSL-Zertifikat selber erstellen. Der einzige Unterschied zu einem offiziellen Zertifikat ist, dass der Webbrowser feststellt, dass es nicht von einer offiziellen Zertifizierungsstelle erstellt wurde. Alle Webbrowser zeigen eine Warnung an, wenn ein solches selbsterstelltes Zertifikat verwendet wird. Die eigentliche Verschlüsselung hingegen ist voll funktionsfähig, d.h. die Zugriffe auf eine mit einem selbsterstellten Zertifikat geschützte Website können ebenso wenig entschlüsselt werden wie die Zugriffe auf eine Website mit einem offiziellen SSL-Zertifikat.

Solche selbsterstellten Zertifikate sollten jedoch keinesfalls für öffentlich zugängliche Webserver verwendet werden, und zwar aus folgendem Grund: Wenn viele SSL-Webseiten selbsterstellte Zertifikate verwenden, dann wird der durchschnittliche Internet-Nutzer der Webbrowser-Warnung keine Bedeutung mehr beimessen, und es tritt ein Gewöhnungseffekt ein.



Mit folgendem Befehl wird ein self-signed certificate erstellt, das für 365 Tage gültig ist:

```
J:\xampp\apache\bin>openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

CRT anzeigen

Mit folgendem Befehl kann festgestellt werden, ob alle Angaben im CSR korrekt sind:

```
J:\xampp\apache\bin>openssl asn1parse -inform PEM -in server.crt
```

Installation des SSL-Zertifikats

Das SSL-Zertifikat wird installiert, indem dem Webserver der Pfad auf das Zertifikat sowie auf den privaten Key mitgeteilt wird. Beim Apache 2.x Webserver ist die SSL-Konfiguration in eine separate Datei ausgelagert, die zunächst einmal in die Konfigurationsdatei `conf/httpd.conf` inkludiert werden muss (ist im Grundzustand auskommentiert):

```
Include "conf/extra/httpd-ssl.conf"



##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
    #   General setup for the virtual host
    DocumentRoot "/xampp/htdocs"
    ServerName localhost:443
    ServerAdmin webmaster@localhost
    ErrorLog "logs/error.log"
    <IfModule log_config_module>
        CustomLog "logs/access.log" combined
    </IfModule>

    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on

    #   SSL Cipher Suite:
    #   List the ciphers that the client is permitted to negotiate.
    #   See the mod_ssl documentation for a complete list.
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

    #   Server Certificate:
    #   Point SSLCertificateFile at a PEM encoded certificate.  If
    #   the certificate is encrypted, then you will be prompted for a
    #   pass phrase.  Note that a kill -HUP will prompt again.  Keep
    #   in mind that if you have both an RSA and a DSA certificate you
    #   can configure both in parallel (to also allow the use of DSA
    #   ciphers, etc.)
    #SSLCertificateFile "conf/ssl.crt/server-dsa.crt"
    SSLCertificateFile "conf/ssl.crt/server.crt"

    #   Server Private Key:
    #   If the key is not combined with the certificate, use this
    #   directive to point at the key file.  Keep in mind that if
    #   you've both a RSA and a DSA private key you can configure
    #   both in parallel (to also allow the use of DSA ciphers, etc.)
    #SSLCertificateKeyFile "conf/ssl.key/server-dsa.key"
```

```
    SSLCertificateKeyFile "conf/ssl.key/server.key"
```

…

Quellen:

https://www.schirmacher.de/display/INFO/Apache+SSL+Zertifikat+erstellen

http://www.dylanbeattie.net/docs/openssl_iis_ssl_howto.html

http://aktuell.de.selfhtml.org/artikel/server/apacheconf/

http://www.openssl.org/

FAQ

The root issue is that the RANDFILE variable in the OpenSSL configuration file is ignored on Windows. This has been a long-standing problem that continues to exist as of the OpenSSL v1.0a release, regardless of whether the target Windows platform is x86 or x64.

There is a delightfully simple solution, though. Merely use a regular environmental var to set the RANDFILE value, like

```
set RANDFILE=.rnd
```

D. A. Waldvogel, 06.12.2011
M133_Zertifiakte_Apache.docx