

Einrichtung einer sicheren https Verbindung

Um eine sichere Verbindung einzurichten muss im Apache ein neuer virtueller Host eingerichtet werden.

Voraussetzungen

Es wird ein **Zertifikat** und ein **privater Schlüssel** im **PEM-Format** (BASE64 kodierte Zeichenkette) benötigt.

Außerdem muss das Zertifikat mit mindestens dem **SHA-256** Signaturalgorithmus signiert sein.

“ All major webbrowser vendors ceased acceptance of SHA-1 SSL certificates in 2017.

Microsoft has discontinued SHA-1 code signing support for Windows Update in August 7, 2020.

- [Wikipedia \(SHA-1\)](#)

Ein Zertifikatsspeicher (PFX / PKCS#12) kann ebenfalls verwendet werden.

Dazu muss das Zertifikat in seine Einzelteile (Zertifikat, privater Schlüssel und ggf. der Zertifikatskette) zerlegt werden.

Extraktion eines PFX-Zertifikatsspeicher

Am Ende der Voraussetzungen, steht mindestens das Zertifikat und der private Schlüssel zur Verfügung.

Ein Beispiel eines Zertifikats:

```
cert_www.toutpourlabiere.com.txt - Editor
Datei Bearbeiten Format Ansicht ?
|-----BEGIN CERTIFICATE-----
MIIF0DCBBLIqAwIBAgIQCBRqCvF8jI3hYlKTt/XkjANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSw5jMRkwFwYDVQQLEwB3
d3cuZGlnaWNaW1cnQyY29tMR0wGwYDVQQDEwRSYXBPZFNNTCBSU0EgQ0EgMjAxODAE
Fw0xODAzMTkwMDAwMDBAFw0xOTA0MTgxMjAwMDBAIExIDAEgNVBAMTF3d3dy50
b3V0cG91cmxhYm11cmUuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAsNPwm1SYVKZmuvpUgpb6DUY+E9D46kXQrDmcufEE5mxeTU0xxftQN9Ze8KMc
FubPHh1t1oXJIBnaPXZj7xzEZq2JIMdmJIOjNATkVIkIHuXYkAmgRnXLCeJNG0C
XgxPsOnHQNY6AMGrjy7EqMS7BL+DMLNgM/1BnUX1sZWxBysoRv+09GJAXA8Q4SY
rkON1GRxhe6w/HdPpbz1hhQ880dLPS5zpzAnsw+xc0K+dmmC0SH2HihJ319C0/gX
wQdfNPL+oXcoS7I2MiRe/9jmEnsa6040Ev+FV0uS4Xxh4HFN6XQbYKv6RZHGJpmz
1zg6k3cF8F8WIKNRw0U/68anHQIDAQABo4ICxDCCAsAwHwYDVR0jBBgwFoAUU8oX
WfxrWAMhLxqu5KqoHIJW2nUwHQYDVR00BBYEFiHe0a4cLnqdwjwZgK/vWz1Jgzo
MDcGA1UdEQQwMC6CF3d3dy50b3V0cG91cmxhYm11cmUuY29tghN0b3V0cG91cmxh
Ym11cmUuY29tMA4GA1UdDEB/wQEAwIFoDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYI
KwYBBQUHAwIwPgYDVR0fBDcwNTAzoDGL4YtaHR0cDovL2NkC5yYXBpZHNzbC5j
b20vUmFwaWRTU0xSU0FQDTIwMTguY3J3MEwGA1UdIARFMEMwNwYJYIZIAyB9bAEC
MCowKAYIKwYBBQUHAgEWHGh0dHBz018vd3d3LmRpb21jZXJ0LmNvbS9DUFMwCAYG
Z4EMAQIBMHUGCCsGAQUFBwEBBgkwZzAmBggrBgEFBQcwAYYaaHR0cDovL3N0YXR1
cy5yYXBpZHNzbC5jb20wPQYIKwYBBQUHMAKGMMWh0dHA6Ly9jYWNlcnRzLnJhcG1k
c3NsLmNvbS9SYXBPZFNNTTFTJQUUNBMjAxOC5jcncwCQYDVROTBAlwADCCAQQGCisG
AQQB1nkCBAIEgfUEgfIA8AB2AKS5CZC0GFgU7sTosxncAo8NZgE+RvfuON3zQ7I
DdwQAAABYj1nkg4AAAQDAECwRQIGUwyNIIs+5xL5AtH9xjIyqWmukjdd/Skj0XqcI
3zQpDQGCIQCrG1hoSfe73JwM2pTN9FH81vv40Z/+BUvVQzSUYJiivQB2AG9Tdqwx
8DEZ2JkApFEV/3cVHBHZAseAKQaNsGian9kTAAABYj1nk5wAAAQDAECwRQIHAIJZh
Yrz4WuWaeBGu/bYy/SwtfjAG9NNzg9aMMcVr1xzZAIhAg000aonVP4yeXfudW+/
tpEgtUQ902+3eiTvJfrxVjANBgkqhkiG9w0BAQsFAAOCAQEAL+I/Esppz2VS1pGz
GtN1i+3ki/7p2qS0DjBfBdTzVn3PNKR1sNCWvoeQ8vqxw/uZbY1hGJh/jpcgjSkG
h3FL1NT/RTZPycTyKjHqcL2mscVXSkWfc7zm3v4/tHA+Q/gvjoH1Nx7mo+r6PI0S
47Eu3b3wQ8f7dt4+RYJrq3r01S36PbMqU5Cx4Sm6b0JHarBo0gggho/YdiEgTx70C
IFHmq5RHRvEmOQvFeK8D3/4D9G1IY4mZ5u1InNy6/tcz+AGgcYXU1N0oAnM5Yk00
FIUNR+2nmerW5959YeDEIot6p++aD2T91WmMYZelB6uzCW53+Gw5IyYxZbuZWGpd
OBcZ5g=====END CERTIFICATE-----
```

Sobald die Dateien vorliegen kann mit der Einrichtung des Virtuellen Hosts begonnen werden.

Konfiguration Webserver

httpd-vhosts.conf - Konfiguration

Das Zertifikat, den privaten Schlüssel des Zertifikats sowie eine etwaige Zertifikatskette unter dem Apache Konfigurationsordner `|SQUEEZE\apache\conf\ssl|` ablegen.

httpd-vhosts.conf - Konfiguration

Der virtuelle Host für den SSL Port `|*: 443|` muss in der Datei `|SQUEEZE\apache\conf\extra\httpd-vhosts.conf|` eingetragen werden.

Die `|vhosts.conf|` Konfiguration muss in der `|httpd.conf|` geladen werden, damit die `|vhosts|` in der Konfiguration des Webserver berücksichtigt werden (bei SQUEEZE bereits eingerichtet).

```
<VirtualHost *: 443>
    ServerName host.domain.net
```

```
ServerAdmin admin@host.domain.net
ServerSignature Off
SSLEngine on
SSLCertificateFile "conf/ssl/server.crt"
SSLCertificateKeyFile "conf/ssl/server.key"
SSLCertificateChainFile "conf/ssl/fullchain.pem"
# DER FOLGENDE TEIL WIRD NUR BEI EINEM PROXY BENÖTIGT
# SSLProxyEngine On
# SSLProxyVerify none
# SSLProxyCheckPeerCN off
# SSLProxyCheckPeerName off
# SSLProxyCheckPeerExpire off
</VirtualHost>
```

Die Pfade zum Zertifikat, den privaten Schlüssel des Zertifikats sowie eine etwaige Zertifikatskette sind entsprechend zu setzen.

Der **host.domain.net** Wert ist durch den entsprechenden Hostnamen zu ersetzen.

Zuletzt den Virtuellen Host (`|VirtualHost *:80|`) auskommentieren.

httpd.conf - Konfiguration

Der Webserver muss nun auf den SSL (HTTPS) Port hören.

Dies stellen wir in der Date `|apache\conf\httpd.conf|` ein.

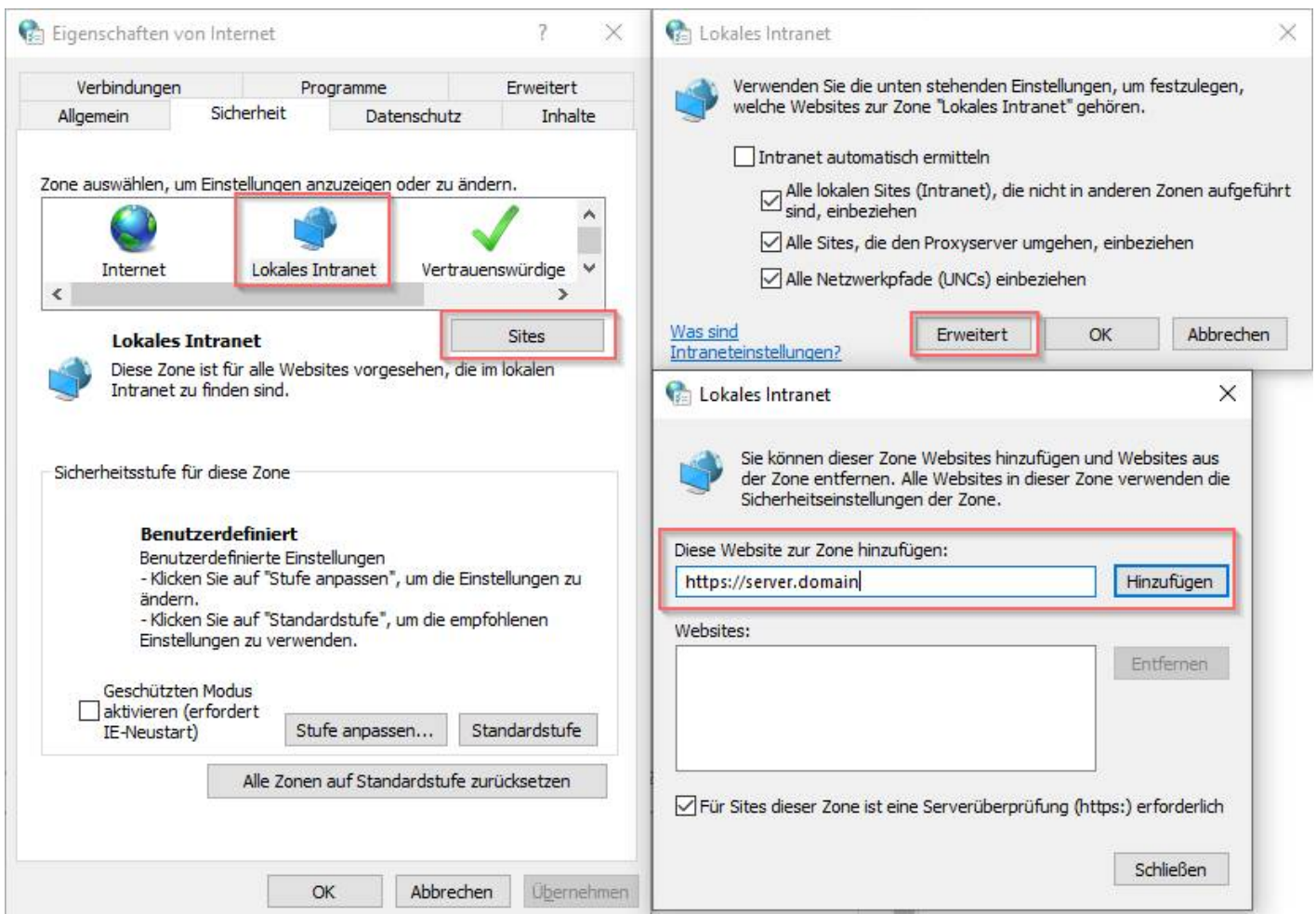
```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
Listen 443
```

Weiter unten in der Konfigurationsdatei müssen wir noch das SSL Modul suchen und dieses einkommentieren.

Troubleshooting

Die Seite kann auf den Clients nicht aufgerufen werden?

Handelt es sich um eine Intranet-Domäne (`[*.local]` bspw.), dann muss die Server FQDN (URL) (<https://servername.domäne>) in den Internetoptionen der Clients bei den Intranetsites hinzugefügt werden. Sollte dies nicht funktionieren, ist die Seite bei den Vertrauenswürdigen Sites unterzubringen.



Seit den Windows Servern 2019 (und Windows 10) sind die TCP Ports `443`, `8443` in der Firewall standardmäßig nicht freigegeben.

Dazu sind also entsprechende eingehende und ausgehende Firewallregeln zu definieren.

Extraktion eines PFX -

Zertifikatsspeicher

Wenn das Zertifikat, die Zertifikatskette sowie der private Schlüssel (ohne Passphrase) für den Apache Webserver als Zertifikatsspeicher (PFX / PKCS#12) vorliegt, kann diese Batch (ohne jegliche Gewährleistung) ausgeführt werden, um an die notwendigen Einzelteile zu gelangen.

Dazu werden die [OpenSSL Binaries](#) benötigt (seit SQUEEZE 1.10 ausgeliefert).

Setzen der Batch-Variablen

Es müssen im Batch-Script die folgenden Variablen gesetzt werden, damit das Script fehlerfrei arbeiten kann.

```
SET OPENSSL=D: \DEXPRO\TOOLS\OPENSSL\openssl.exe

SET PFXFILE=D: \DEXPRO\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx
SET OUTPUTFOLDER=D: \DEXPRO\ZERTIFIKATE\OUT\
SET OUTPUTFILENAME=KONVERTIERTES_KUNDENZERTIFIKAT

SET REMOVEPASSPHRASE=true
```

Dabei werden die Pfade zu OpenSSL, dem Ausgabeordner und dem PFX Zertifikatsspeicher (PFX), sowie die Namen der zu erstellenden Zertifikatsbestandteile angegeben. Damit der private Schlüssel von etwa dem Apache Webserver gelesen werden kann, muss der private Schlüssel ohne PEM-Passphrase vorliegen. Dazu kann das Flag `REMOVEPASSPHRASE=true` gesetzt werden.

Ausführen der Batch

Einfach den Anweisungen der Batch-Datei folgen:

```
C:\Windows\System32\cmd.exe

-----
EXTRACTION OF THE INDIVIDUAL COMPONENTS OF A PFX CERTIFICATE STORE
Setting the variables ...
  openssl.exe: [C:\OPENSSL\openssl.exe]
  PFX certificate store: [C:\Users\Dexpro\Desktop\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx]
  Destination folder: [C:\Users\Dexpro\Desktop\ZERTIFIKATE\OUT\]
  Destination file name: [KONVERTIERTES_KUNDENZERTIFIKAT]
-----
Checking the variables ...
  openssl.exe found
  Customer certificate store [C:\Users\Dexpro\Desktop\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx] found
  Destination folder [C:\Users\Dexpro\Desktop\ZERTIFIKATE\OUT\] found
-----
Start extraction ...
PRIVATE KEY EXTRACTION
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
CERTIFICATE EXTRACTION
Enter Import Password:
CERTIFICATE CHAIN EXTRACTION
Enter Import Password:
REMOVE PEM-PASSPHRASE
Enter pass phrase for C:\Users\Dexpro\Desktop\ZERTIFIKATE\OUT\KONVERTIERTES_KUNDENZERTIFIKAT.key:
writing RSA key
-----
EXTRACTION COMPLETED!
-----
Drücken Sie eine beliebige Taste . . .
```

Ergebnis der Batch (Bestandteile des PFX)

Am Ende der Extraktion sind die folgenden Dateien im definierten Ausgabeordner zu finden:

Dieser PC > Desktop > ZERTIFIKATE > OUT				
	Name	Änderungsdatum	Typ	Größe
🔗	KONVERTIERTES_KUNDENZERTIFIKAT.crt	19.10.2020 18:30	Sicherheitszertifikat	4 KB
🔗	KONVERTIERTES_KUNDENZERTIFIKAT.key	19.10.2020 18:30	KEY-Datei	3 KB
🔗	KONVERTIERTES_KUNDENZERTIFIKAT_chain.pem	19.10.2020 18:30	PEM-Datei	0 KB
🔗	KONVERTIERTES_KUNDENZERTIFIKAT_nopass.key	19.10.2020 18:30	KEY-Datei	2 KB

- Das eigentliche Zertifikat (*.crt)
 - Der private Key (mit PEM-Passphrase) (*.key)
 - Der private Key (ohne PEM-Passphrase) (*_nopass.key)
 - Die Zertifikatskette (*_chain.pem).
- Ist diese Datei leer, so gibt es in dem Zertifikatsspeicher keine auszugebende Kette.

Bei allen Dateien müssen im Anschluss die von OpenSSL generierten Informationen entfernt werden:

```
KONVERTIERTES_KUNDENZERTIFIKAT.ct
1 Bag Attributes
2   localKeyID: 01 00 00 00
3   friendlyName: [REDACTED].com
4   subject=C = DE, ST = Hamburg, L = Hamburg, O = [REDACTED] AG, OU = IT, CN = *. [REDACTED].com
5
6   issuer=C = CH, O = SwissSign AG, CN = SwissSign Server Gold CA 2014 - G22
7
8   -----BEGIN CERTIFICATE-----
9   MIIII [REDACTED]
10  [REDACTED]
11  [REDACTED]
12  [REDACTED]
13  [REDACTED]
14  [REDACTED]
15  [REDACTED]
16  [REDACTED]
17  [REDACTED]
18  [REDACTED]
19  [REDACTED]
20  [REDACTED]
21  [REDACTED]
22  [REDACTED]
23  [REDACTED]
24  [REDACTED]
25  [REDACTED]
26  [REDACTED]
27  [REDACTED]
28  [REDACTED]
29  [REDACTED]
30  [REDACTED]
31  [REDACTED]
32  [REDACTED]
33  [REDACTED]
34  [REDACTED]
35  [REDACTED]
36  [REDACTED]
37  [REDACTED]
38  [REDACTED]
39  [REDACTED]
40  [REDACTED]
41  [REDACTED]
42  [REDACTED]
43  [REDACTED]
44  [REDACTED]
45  [REDACTED]
46  [REDACTED]
47  [REDACTED]
48  [REDACTED]
49  [REDACTED]
50  [REDACTED]
51  [REDACTED]
52  [REDACTED]g=
53   -----END CERTIFICATE-----
54
```

Batch Script Quellcode

Ohne jegliche Gewährleistung oder Anspruch auf Support.

```
@ECHO off
ECHO - - - - -
```

```

REM VARIABLES TO SET!

SET OPENSSSL=D: \DEXPRO\TOOLS\OPENSSSL\openssl.exe

SET PFXFILE=D: \DEXPRO\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx
SET OUTPUTFOLDER=D: \DEXPRO\ZERTIFIKATE\OUT\
SET OUTPUTFILENAME=KONVERTIERTES_KUNDENZERTIFIKAT
REM REMOVE PEM PASSPHRASE? -> TRUE / FALSE
SET REMOVEPASSPHRASE=true

REM START DER EXTRAKTION
ECHO EXTRACTION OF THE INDIVIDUAL COMPONENTS OF A PFX CERTIFICATE STORE
ECHO Setting the variables ...
ECHO [openssl.exe: [%OPENSSSL%]
ECHO [PFX certificate store: [%PFXFILE%]
ECHO [Destination folder: [%OUTPUTFOLDER%]
ECHO [Destination file name: [%OUTPUTFILENAME%]
ECHO      - - - - -
ECHO Checking the variables ...
if exist %OPENSSSL% (
    ECHO [openssl.exe found
) else (
    ECHO [openssl.exe [%OPENSSSL%] not found - please adjust the path!
    goto ERROREND
)
if exist %PFXFILE% (
    ECHO [Customer certificate store [%PFXFILE%] found
) else (
    ECHO [Customer certificate store [%PFXFILE%] not found - please adjust the path!
    goto ERROREND
)
if exist %OUTPUTFOLDER% (
    ECHO [Destination folder [%OUTPUTFOLDER%] found
) else (
    ECHO [Destination folder [%OUTPUTFOLDER%] not found - please adjust the path!
    goto ERROREND
)
if "%OUTPUTFILENAME%"==" " (
    ECHO [No destination filename was specified!
    goto ERROREND

```



```

)
ECHO      - - - - -
ECHO Start extraction ...
ECHO PRIVATE KEY EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -nocerts -out %OUTPUTFOLDER%%OUTPUTFILENAME%. key
ECHO CERTIFICATE EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -clcerts -nokeys -out %OUTPUTFOLDER%%OUTPUTFILENAME%. crt
ECHO CERTIFICATE CHAIN EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -cacerts -nokeys -chain -out
%OUTPUTFOLDER%%OUTPUTFILENAME%_chain.pem

REM REMOVE PEM PASSPHRASE
IF "%REMOVEPASSPHRASE%"=="true" (
[ECHO REMOVE PEM-PASSPHRASE
%OPENSSL% rsa -in %OUTPUTFOLDER%%OUTPUTFILENAME%. key -out
%OUTPUTFOLDER%%OUTPUTFILENAME%_nopass. key
) ELSE (
[ECHO PEM-Passphrase is not removed
)
GOTO END

: END
ECHO      - - - - -
ECHO EXTRACTION COMPLETED!
ECHO - - - - -
PAUSE
EXIT

: ERROREND
ECHO      - - - - -
ECHO EXTRACTION FAILED!
ECHO PLEASE CHECK ALL PARAMETERS!
ECHO - - - - -
PAUSE
EXIT

```

Alternative Konfiguration

Einrichtung des Virtuellen Hosts

In der Datei `D:\SQUEEZE\apache\conf\extra\httpd-vhosts.conf` eintragen:

```
# Alternative Konfiguration:
LoadModule ssl_module modules/mod_ssl.so
<VirtualHost *:8443>
    ServerName host.domain.net
    DocumentRoot "${SQR00T}\htdocs\public"
    <IfModule mod_ssl.c>
        SSLEngine on
        SSLCertificateKeyFile "conf/ssl/package.key"
        SSLCertificateFile "conf/ssl/package.cer"
        SetEnvIf User-Agent ".MSIE.*" \
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0
    </IfModule>
</VirtualHost>
```

Der **host.domain.net** Wert ist durch den entsprechenden Hostnamen zu ersetzen.

Revision #10

Created 15 June 2020 11:07:14 by Phillip Langer

Updated 5 March 2021 10:32:12 by Maximillian Weitze