SoftENGINE

Kaufmännische Software für Handel, Industrie und E-Commerce

WEBWARE 2.10

Dokumentation

Zertifikate

in der

WEBWARE

04.09.2017

V 2.04

INHALTSVERZEICHNIS

Schnell Übersicht: "Kein Zertifikat-Fehler"

Warum ein Zertifikat ?

Um einen WEBWARE-Server mit sicherer Kommunikation betreiben zu können, wird ein gültiges Server-Zertifikat benötigt.
Beim Zugriff mit einem Browser wird dieses Zertifikat an den Browser übertragen und für die Prüfung des WEBWARE-Server verwendet. Wird dabei ein Zertifikat als nicht gültig bzw. abgelaufen usw. erkannt, zeigt der Browser eine Fehlerseite, welche den Anwender warnt, diesen Server zu verwenden.

Ein Zertifikat ist also so etwas ähnliches wie ein Ausweis den Sie den Client's (Browsern) beim Verbindungsaufbau vorlegen müssen. Dieses Zertifikat wird dabei für einen Domain-Namen (Bspl: Meine-WEBWARE.de) ausgestellt. Der Client (Browser) prüft nach Erhalt des Zertifikat die Gültigkeit, die Gültigkeitsdauer (Start-Termin/End-Termin) und auch, ob der im Zertifikat angegebene Domain-Namen mit dem Domain-Namen der in der Browser Adressleiste eingegeben wurde übereinstimmt.

Aktivierung eines gültigen WEBWARE-Zertifikats

Wir haben Ihrem WEBWARE-Server ab 30.06.2015 ein zusätzliches Zertifikat bei gelegt.

Meine-Webware.de

Mit diesem Zertifikat können Sie nach Anpassung der HOSTS-Datei oder Einsatz eines eigenen Name-Servers mit

https:// Meine-Webware.de

ohne Zertifikatsfehlermeldung auf Ihre WEBWARE zugreifen. Näheres zur Konfiguration finden Sie in den folgenden Abschnitten dieses Dokuments.

Erstellung eines eigenen Zertifikates

Es gibt einige Zertifizierungsstellen bei denen eigene globale Zertifikate, auch Kostenlos, erstellt werden können. Hierzu finden Sie nähere Informationen in den folgenden Abschnitten.

Welche Zertifikate liefert die WEBWARE mit ?

Für den Betrieb eines WEBWARE Server wird ein SSL-Zertifikat benötigt. Wir liefern mit dem WEBWARE-Server 2 Zertifikate aus.

- Demozertifikat (neu ab 02.07.2016, gültiges Chain-Zertifikat für Domain meine-webware.de)
- Meine-Webware.de (neu ab 02.07.2016, gültiges Chain-Zertifikat..)
- Neue Let's Encrypt Zertifikats Erfstellung/Verwaltung (Neu ab 13.02.2017)

In der Folge wird beschrieben, wie diese Zertifikate eingesetzt werden können, bzw. wie Sie bei Problemen oder der Einführung eigener Zertifikate vorgehen sollten.

WEBWARE Zertifikat

Einleitung

Ein Zertifikat ist direkt an eine Adresse (Bspl: SoftEngine.de oder 192.168.99.99..) gebunden. Daher ist es nicht möglich ein Generelles Zertifikat auszuliefern das für alle Umgebungen passt.

Damit ein gültiges Zertifikat in einem Browser akzeptiert wird, ist es notwendig das das Zertifikat von einer, dem Browser bekannten Stelle (CA), signiert (unterschrieben) wird. Der Browser prüft dabei die Kette von Zertifikaten bis zur Bekannten Stelle (CA).

Achtung!!: Bei einer Fehlkonfiguration ist der Zugriff auf Ihre WEBWARE nicht mehr möglich, da die WEBWARE ein funktionierendes Schlüsselsystem voraussetzt. Falls Ihre WEBWARE nicht mehr ansprechbar ist, fügen Sie folgende Zeilen in Ihre WWS.ini ein:

```
BWWSSL_CA_ZERTIFIKAT=demozertifikat\ca.pem
BWWSSL_ZERTIFIKAT=demozertifikat\server.pem
BWWSSL_PASSWORD4PRIVKEY=
BWWSSL_PRIVATEKEY=demozertifikat\key.pem
BWWSSL_USE_CHAIN_ZERTIFIKAT=J
BWWSSL_CHAIN_ZERTIFIKAT=demozertifikat\chain.pem
```

Ein gültiges Zertifikat besteht aus mehreren Bestandteilen:

CA-Zertifikat:	Verweis auf die signierende Stelle
Server-Zertifikat:	Zertifikat die für Ihren Server ausgestellt wurde
Schlüsseldatei:	In dieser Datei ist der interne und öffentliche Schlüssel für die Verschlüsselung vorhanden
Passwort für Schlüsseldatei:	Damit ein WEB-Server die Schlüsseldatei öffnen kann, benötigen Sie den zugehörigen geheimen Schlüssel. Die WEBWARE erlaubt es Ihnen, diesen Schlüssel über die WWS.ini vorzugeben.

Chain-Datei (optional) in der eine "Kette" von Zertifikaten enthalten ist.

HINWEIS: Nach erfolgreicher Konfiguration kann der Eintrag
#-INIOK-# BWWSSL_PASSWORD4PRIVKEY=xx

aus der WWS.INI Datei entfernt werden, da der Schlüssel in der internen Parameterverwaltung gespeichert wird, und Ihr geheimer Schlüssel damit nicht auslesbar ist.

Möglichkeiten, um die WEBWARE mit einem gültigen Zertifikat auszustatten

Verwendung von SoftENGINE ausgelieferten Zertifikaten

Falls Sie keine Änderung in der Konfiguration vornehmen ist das Standard-Zertifikat Meine-Webware.de als Standard im WEBWARE-Server installiert. Nähere Infos finden Sie in der Datei

\bin\wws\demozertifikat\liesmich.txt

Damit das Zertifikat von Ihrem Browser akzeptiert wird müssen Sie folgende Schritte durchführen.

- Mit Hilfe eines Proxy's/Router/Name-Server oder der lokalen HOST-Datei muss der Domain Name des Rechners auf Meine-Webware.de gesetzt werden. Sie können dann vom Browser aus mit der Adresse https://meine-webware.de auf die WEBWARE zugreifen
- Das Zertifikat ist ein öffentliches Zertifikat das von allen gängigen Browsern akzeptiert wird.
- Das Zertifikat ist gültig bis 03.12.2017
- Bei Vorgabe über HOSTS-Datei ist der Zugriff nur lokal möglich. Bei Verwendung eines Named-Server ist auch der Zugriff von anderen Rechnern die diesen Name-Server verwenden ohne Zertifikats-Fehler möglich.

Anpassung einer bestehenden WWS.INI bei Update eines bestehenden Systemes.

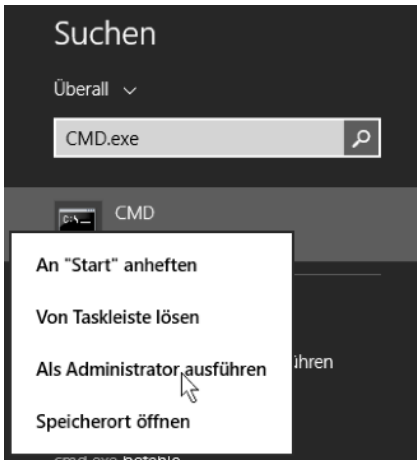
(ersetzen Sie hier [WWS-PFAD] mit dem Verzeichnispfad des WW-Servers, bzw. wenn die Zertifikatsdatei unterhalb des WWS-Pfades liegt [bin\wws] kann direkt mit dem Zertifikatspfad begonnen werden)

```
BWWSSL_ON=J
BWWSSL_CA_ZERTIFIKAT=demozertifikat\ca.pem
BWWSSL_ZERTIFIKAT=demozertifikat\server.pem
BWWSSL_PASSWORD4PRIVKEY=""
BWWSSL_PRIVATEKEY=demozertifikat\key.pem
BWWSSL_USE_CHAIN_ZERTIFIKAT=J
BWWSSL_CHAIN_ZERTIFIKAT=demozertifikat\chain.pem
```

Einsatz auf einem lokalen System, durch Anpassen der HOSTS Datei

Gehen Sie hierzu wie folgt vor, da die Änderung der Datei HOSTS nur von einem Admin möglich ist:

Geben Sie in der Windows-Suche den Begriff „CMD.exe“ ein und starten Sie das gefundene Programm über "als Administrator ausführen"



Wechseln Sie in das Verzeichnis cd c:\windows\system32\drivers\etc

Öffnen Sie in einem Text-Editor die Datei HOSTS (hat keine Datei-Endung)

Fügen Sie nun am Ende der Datei die folgende Zeile ein

127.0.0.1 meine-webware.de

(Hinweis, falls Ihnen ihre Lokale IP-Adresse bekannt ist, können Sie auch diese hier angeben, wenn nicht, ist diese mit dem Befehl ipconfig in einer Kommandozeile ermittelbar)

Speichern Sie die Datei ab und beenden Sie die Kommando-Zeile (CMD.exe)

Fertig: Nun müsste die WEBWARE als sichere Seite unter der Adresse https://meine-webware.de erreichbar sein.

Erstellen eines kostenlosen Zertifikat über StartSSL.com

!!! Ab Februar 2017 werden von einigen Browser-Hersteller (CHROME/FIREFOX) Zertifikate von STARTSSL.com nicht mehr akzeptiert. !!!

Es ist möglich bei der Zertifizierungsstelle https://www.startssl.com/ kostenlose Zertifikate zu beantragen. Diese Zertifikate sind 1 Jahr gültig. Es ist nur möglich ein Zertifikat für eine Domain zu beantragen bei der man Zugriff auf eine von 3 Haupt-eMail-Adressen hat.
Bspl:

- webmaster@softengine.de
- postmaster@softengine.de
- hostmaster@softengine.de

Konfiguration des WW-Servers für StartSSL Zertifikate
Um den WW-Server in allen Browsern korrekt mit den Start-SSL Zertifikaten verwenden zu können, muss ein sogenanntes Chain-Zertifikat erstellt werden.
Dabei muss innerhalb einer Datei der Zertifizierungspfad der einzelnen Zertifikate enthalten sein. Die Chain-Datei muss im PEM-Format vorliegen. Ein Beispiel für ein Chain-Zertifikat finden Sie im Pfad bin\wws\meine-webware.de bzw. bin\wws\demozertifikat.

Link auf einen Artikel der die Erstellung erklärt:
http://www.heise.de/security/artikel/SSL-fuer-lau-880221.html

Link auf einen Artikel der erklärt wie man die Chain-Datei unter Unix erstellt
http://jasoncodes.com/posts/startssl-free-ssl

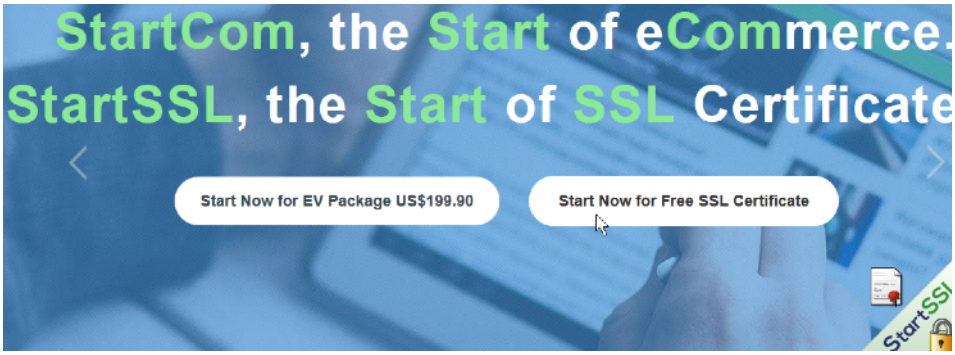
Schritt für Schritt Erklärung Anlage eines Zertifikates

Um ein eigenes Zertifikat mit Hilfe von STARTSSL zu erzeugen benötigen, Sie die Datei OpenSSL.exe welche von der WEBWARE im bin\wws Pfad mit ausgeliefert wird.

Für dieses Beispiel verwende ich meine-webware.de als Zieldomain.

1. Anmelden bei STARTSSL

Gehen Sie hierzu auf die Seite STARTSSL.com und melden Sie sich mit "Sign Up" dort an.



Wichtig ist, das Sie zu einer der 3 eMail Adressen Ihrer Domain Zugriff haben: webmaster@.., postmaster@.., oder hostmaster@..., um sich selbst zu Authentifizieren.

2. Erzeugen eines CSR (Certificate Signing Request)

Hierzu benötigen Sie die „OPENSSL.exe“. Ein CSR ist ein Text der später an STARTSSL.com übergeben wird und bei dem alle notwendigen Informationen enthalten sind.

Ersetzen Sie in dem Aufruf den Text *„meine-webware.de"* mit Ihrer Domain

openssl req -newkey rsa:2048 -keyout meine-webware.de.key -out meine-webware.de.csr

In der Folge werden sie aufgefordert, einige Informationen einzugeben:

Wichtig ist, bei “Enter PEM Pass Phrase" ein Passwort für die Schüsseldatei einzugeben.

```
D:\>openssl req -newkey rsa:2048 -keyout meine-webware.de.key -out meine-webware.de.csr
Generating a 2048 bit RSA private key
.....................................................................................
.......+++
writing new private key to 'meine-webware.de.key'
Enter PEM pass phrase:  meinewebware
Verifying - Enter PEM pass phrase: meinewebware
-----
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]:Wohnort
Locality Name (eg, city) []:Wohnort
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Meine-Firma
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:meine-webware.de
Email Address []:

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

Nachdem die Erzeugung abgeschlossen ist, erhalten Sie 2 Dateien.

```
02.07.2016  09:25             1.037 meine-webware.de.csr
02.07.2016  09:25             1.834 meine-webware.de.key
```

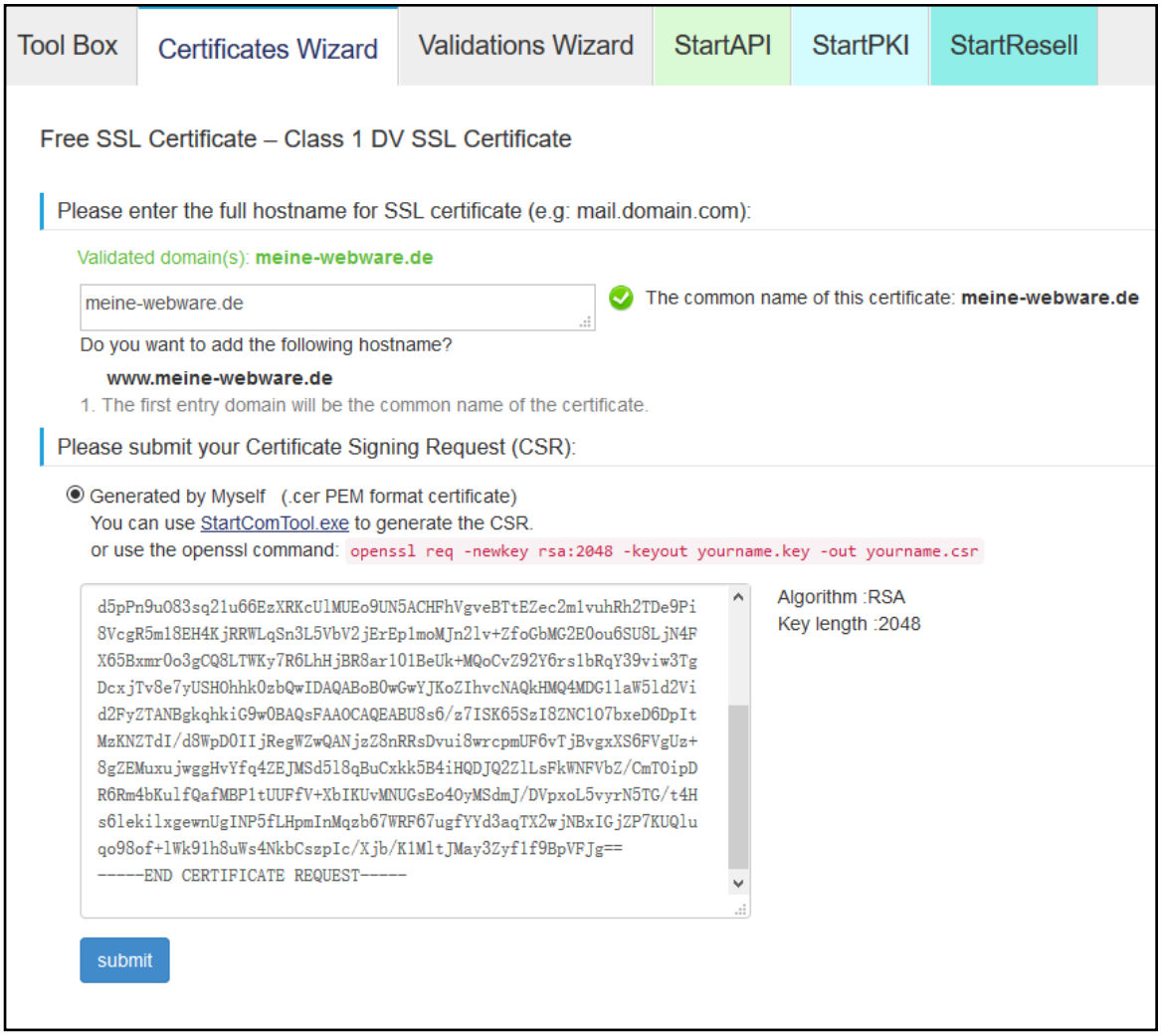
Die *„meine-webware.de.key“* ist der geheime Schlüssel, der später im WW-Server benötigt wird. (Hierzu gehört auch das vergebene Passwort).

Die zweite Datei ist der CSR, welcher für die Zertifikats-Anfrage benötigt wird.

3. Wechseln Sie nun zu STARTSSL.COM

Melden Sie sich an, und Validieren Sie Ihre Domain. Dabei wird für die Domain und auch für die von Ihnen dort einzugebende eMail-Adresse ein Authentification-Code geschickt mit dem Sie sich einmalig authentifizieren müssen.

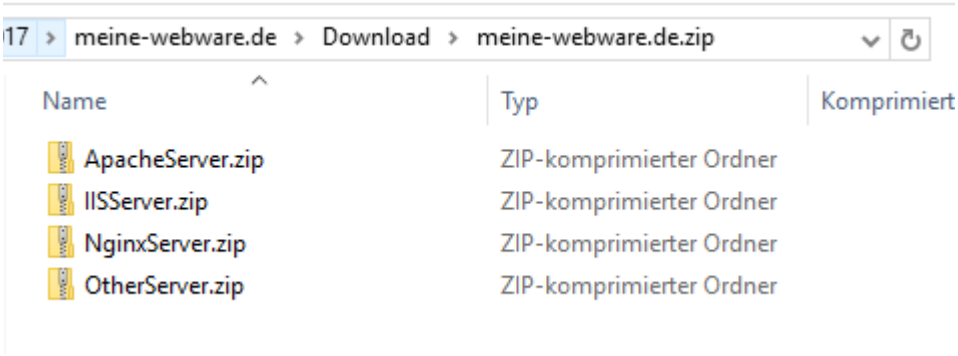
4. Wechseln Sie dann in den Bereich Certificates Wizard



Geben Sie Ihre Domain ein (meine-webware.de), markieren Sie den Radio-Button (Generated by Myself), und kopieren Sie die CSR-Datei mittels Copy&Paste in den Eingabeeditor.

Senden Sie dann die Abfrage mit „Submit“ ab.

Sie erhalten dann einen Link, mit dem Sie eine ZIP-Datei herunterladen können. Diese besteht aus mehreren ZIP-Dateien. Hier ist die Datei OtherServer.zip wichtig. Entpacken Sie diese in ein Verzeichnis:



5. Erzeugen der CHAIN-Datei

Wechseln Sie in das Verzeichnis in der Sie die Dateien aus OtherServer.zip kopiert haben. Dort kopieren Sie folgendendes Script mit als Batch-Datei ein (Bspl. Mache.BAT)

REM Kopieren der Meine-webware.de Zertifikate in eine Chain-Datei

type 2_%1.crt > %1.crt

type 2_%1.crt > startssl.chain.class1.server.crt

type 1_Intermediate.crt >> startssl.chain.class1.server.crt

type root.crt >> startssl.chain.class1.server.crt

type root.crt > startssl.ca.crt

Rufen Sie anschließend die Mache.Bat dem Aufrufparameter Ihrer Domain auf. Beispiel:

MACHE.BAT meine-webware.de

Damit wird nun eine Chain-Zertifikatsdatei mit dem Namen startssl.chain.class1.server.crt erstellt.

Sie verfügen nun über alle Dateien, die Sie für das Zertifikat benötigen.

Kopieren Sie nun folgende Dateien in ein Verzeichnis, welches Sie zuvor unterhalb des BIN\WWS-Verzeichnisses für Ihre Domain anlegen. (Bspl: meine-webware.de)

In diesem sollten dann folgende Dateien enthalten sein.

- startssl.ca.crt
- meine-webware.de.crt
- meine-webware.de.key (wurde zuvor von uns selbst erstellt und muss selbst kopiert werden)
- startssl.chain.class1.server.crt

Nun müssen Sie das Zertifikat noch im WW-Server bekannt machen. Das kann mit Hilfe des System-Cockpits oder wie hier gezeigt, durch die Angabe in der WWS.ini erfolgen.

Fügen Sie hierzu folgende Zeilen in die WWS.ini ein:

```
BWWSSL_CA_ZERTIFIKAT=meine-webware.de\startssl.ca.crt
BWWSSL_ZERTIFIKAT= meine-webware.de \ meine-webware.de.crt
BWWSSL_PASSWORD4PRIVKEY=meinewebware
BWWSSL_PRIVATEKEY= meine-webware.de \private-key.key
BWWSSL_USE_CHAIN_ZERTIFIKAT=J
BWWSSL_CHAIN_ZERTIFIKAT= meine-webware.de \startssl.chain.class1.server.crt
```

Nach einem Neustart des WW-Servers sollte dann das Zertifikat eingelesen und verwendet werden.

Erstellung eines eigenen, selbst Signierten Zertifikates

Mit Hilfe der OpenSSL - Programme können Sie sich auch ein selbst signiertes Zertifikat erstellen. Das von SoftENGINE ausgelieferte demo.webware.de Zertifikat ist ebenfalls mit openSSL erstellt.

Hier ein Link zu einer Einleitung in Zertifikate:

http://www.openssl.org/docs/HOWTO/certificates.txt

Hier ein Link zu einer Kurz Referenz von OpenSSL

http://www.dfn-cert.de/informationen/themen/verschluesselung_und_pki/openssl-kurzreferenz.html

Hier ein YouTube Video

http://www.youtube.com/watch?v=LHUbQtUeQ0o

Let's Encrypt: Erstellen von WEBWARE Zertifikaten

Bei der integrierten Zertifikats Verwaltung über „Let's Encrypt“ ist zu beachten, dass es sich um einen externen Anbieter handelt, dessen Dienstleistung nicht von SoftENGINE garantiert werden kann

https://letsencrypt.org/

Die WEBWARE ermöglicht Ihnen, integrierte Zertifikate mit Hilfe der WEB-Platform „Let's Encrypt“ (im folgenden LE benannt) zu erstellen und zu verwenden. Dies kann direkt aus dem WEBWARE System-Cockpit erfolgen. Um diese Funktion zu verwenden, sind einige Grundvorrausetzungen zu erfüllen.

Ein erstelltes Zertifikat muss von LE überprüft und die Berechtigung der Verwendung getestet werden. Hierzu benötigt die LE-Zertifikatsprüfung die Möglichkeit zu ermitteln, ob Sie die Hoheit / Berechtigung über die Domain bzw. Subdomain haben für die Sie ein Zertifikat erstellen wollen.

WEBWARE Zertifikats - Prüfungsverfahren

Die WEBWARE bietet Ihnen 2 Verfahren an mit denen Sie die die Prüfung auf Berechtigung für Ihre Domian durchführen können. (HTTP und FTP)

HTTP-Prüfung

Hier sind 2 Voraussetzungen zu erfüllen. Der Rechner auf dem die WEBWARE betrieben wird, muss aus dem Internet unter dem zu prüfenden Domain-Namen sowie dem HTTP-Port 80 ansprechbar sein. Eine weitere Voraussetzung ist, dass auf dem Rechner ein HTTP-Server auf Port 80 von der WEBWARE gestartet werden kann, welcher aus dem Internet auch über den Domain-Namen ansprechbar ist.

Bsp.: Wunsch-Domain Meine-WEBWARE.de, hier sollte während der Domain-Prüfung der Zugriff mit http://Meine-WEBWARE.de auf den WEBWARE Rechner möglich sein. (HTTP = Port 80)

Hier ist der Grundablauf so, dass das Zertifikat angefordert wird und der Zertifikats-Austeller (LE) eine Anweisung gibt, eine Datei in einem bestimmten Pfad unter http://Meine-WEBWARE.de bereit zu Stellen. Kann dieser dann diese Datei über das Internet herunterladen, wird das Zertifikat erteilt. Die WEBWARE startet hierzu einen HTTP-Server auf Port 80 über den der Zertifikats-Aussteller (LE) die gewünschte Prüfungsdatei laden kann.

Falls Sie einen Proxy vor Ihren WEBWARE-Server geschaltet haben, können Sie den externen Port 80 (HTTP) auch auf einen anderen internen Port auf dem WEBWARE-Server Rechner routen und mit der WW dort temporär einen HTTP-Server für die HTTP-Challenge starten. Hierzu können Sie den Parameter HTTP abweichender Port 80 verwenden.

FTP-Prüfung
Die WEBWARE bietet ein weiteres Verfahren, bei dem die Voraussetzung ist, dass Sie die Zugangsdaten zum Ftp-Server Ihrer Wunsch-Domain haben.

Notwendige Informationen:

FTP-Server Adresse: ftp://meine-webware.de/www/

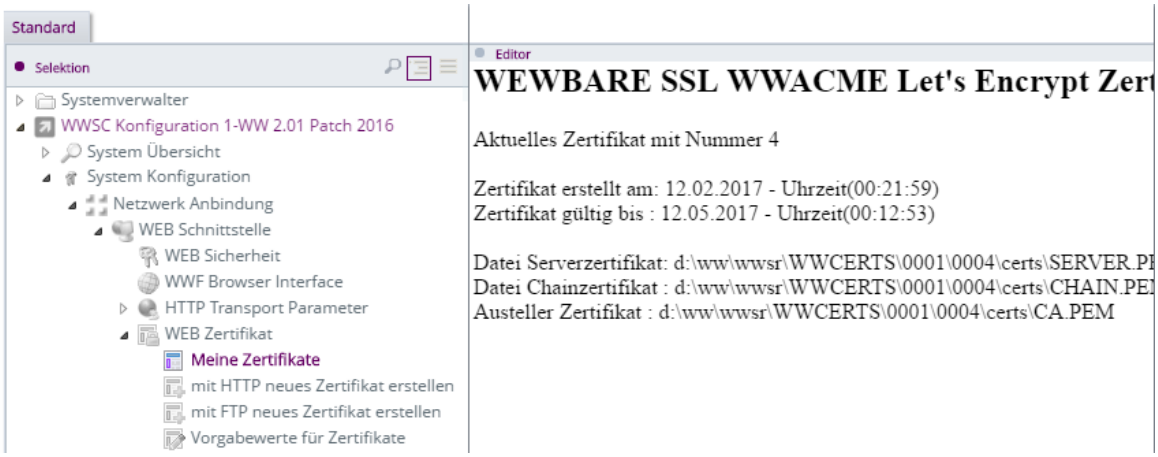
FTP-Server Benutzer: mein_Benutzer..

FTP-Server Passwort: *******

Hier ist der Grundablauf so, dass das Zertifikat angefordert wird und der Zertifikats-Aussteller (LE) eine Anweisung gibt, eine Challenge-Datei in einem bestimmten Pfad unter http://Meine-WEBWARE.de bereit zu stellen.
Kann dieser dann diese Datei über das Internet herunterladen, wird das Zertifikat erteilt. Die WEBWARE kopiert die Challenge-Datei vor der Prüfung in den gewünschten Pfad auf dem FTP-Server, so dass Ihr Standard-Webserver diese ausliefern kann.

Integrierte Zertifikats Verwaltung

Sie finden die Integrierte Zertifikats Verwaltung im Bereich Konfiguration. Unterhalb der WEB Schnittstelle gibt es dort einen Eintrag WEB-Zertifikate unter diesem wird das aktuelle Zertifikat angezeigt.

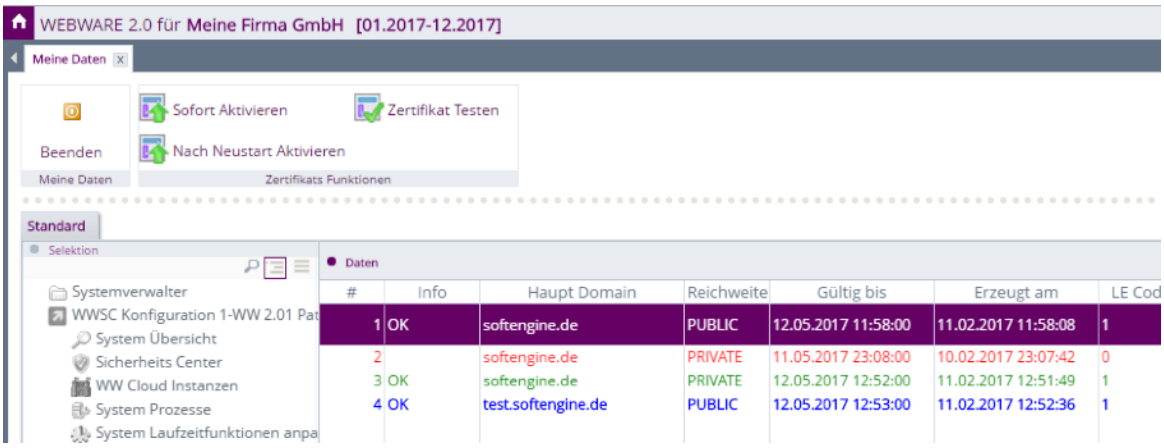


Unterhalb finden sie 4 Äste mit folgenden Aufgaben.

- Meine-Zertifikate: Liste Ihrer mit WEBWARE erstellten Zertifikate
- mit HTTP neues Zertifikat erstellen Ein Zertifikat mit HTTP Prüfung erstellen
- Mit FTP neues Zertifikat erstellen EinZertifikat mit FTP Prüfung erstellen
- Vorgabewerte für Zertifikate Hier werden Vorschlagswerte zwischengespeichert

Meine Zertifikate

Hier erhalten Sie eine Liste aller Zertifikate, die bisher in der WEBWARE von Ihnen erstellt wurden. Je nach Zustand des Zertifikates, werden die Zeilen in unterschiedlicher Farbe dargestellt und Sie in Abhängigkeit vom Zustand des Zertifikates weitere Menü-Punkte im Hauptmenü angezeigt.



Code der Farb-Darstellung der Zertifikate:

ROT: Dieses Zertifikat ist nicht gültig und kann nicht verwendet werden.

GRÜN: Dieses Zertifikat hat gültige Zertifikatsdateien und kann unter Berücksichtigung der Gültigskeitsdauer verwendet werden.

BLAU: Dieses Zertifikat wird aktuell verwendet.

Informationsfelder der Zertifikate

Info:	OK, bedeutet es sind die notwendigen Zertifikatsdateien verfügbar
Haupt-Domain:	Für welche Haupt-Domain wurde das Zertifikat ausgestellt
Reichweite:	PRIVATE - Es handelt sich um ein Test-Zertifikat, nicht verwendbar
	PUBLIC - Es ist ein öffentlich gültiges Zertifikat
Gültig bis:	Ein Zertifikat hat ein Verfallsdatum. Hier wird angegeben bis wann das Zertifikat verwendet werden kann.
Erzeugt am:	Der Browser prüft bei einem Zertifikat ebenfalls der Zeitpunkt ab wann das Zertifikat gültig ist. Da die Zertifikate in der WEBWARE in Echtzeit erstellt und verwendet werden können, sollte dieser Termin immer erreicht werden.

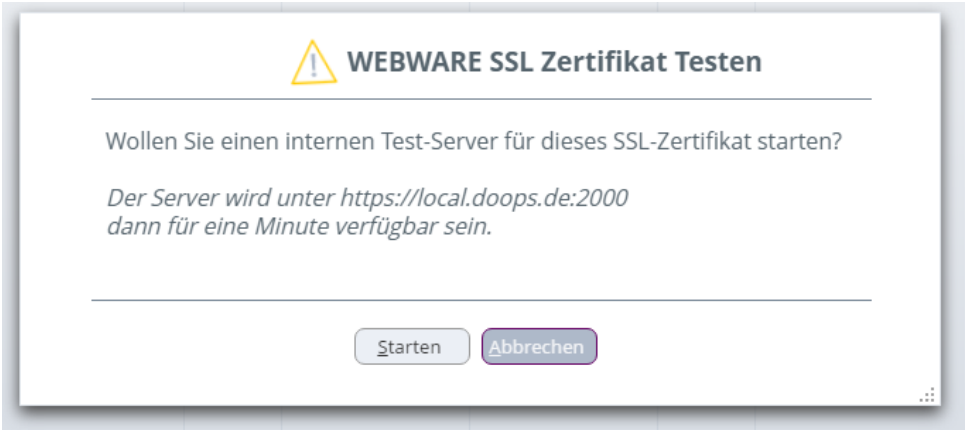
LE-Code	Code von LE der Angibt ob es bei der Erstellung Probleme gab 1=OK)
LE-Informationen	Hier sind weitere Informationen zu finden, falls es Probleme gab
Hinweise	Hinweise vom WWACME Programm welches die Erstellung durchführt
Sub-Domains	Hier sehen Sie die Liste der Sub-Domains welche im Zertifikat enthalten sind

Funktionen für Meine Zertifikate

Markieren Sie ein Zertifikat, so werden Ihnen je nach Zustand verschiedene Funktionen angezeigt. Dies ist davon abhängig um welche Art von Zertifikat (PRIVATE/PUBLIC) es sich handelt und ob das Zertifikat gültig ist.

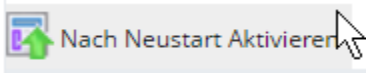
Zertifikat Testen

Wenn Sie ein Zertifikat testen wollen, können Sie dies mit dieser Funktion tun. Dabei wird ein interner Test-Zugang für eine Minute gestartet der das Zertifikat bereit stellt. Die Netzwerkkarte für den Zugang wird dabei aus der aktuellen WEBWARE-Instanz geholt. Beim Port wird ein offener, ausgehend von Port 2000 gesucht.



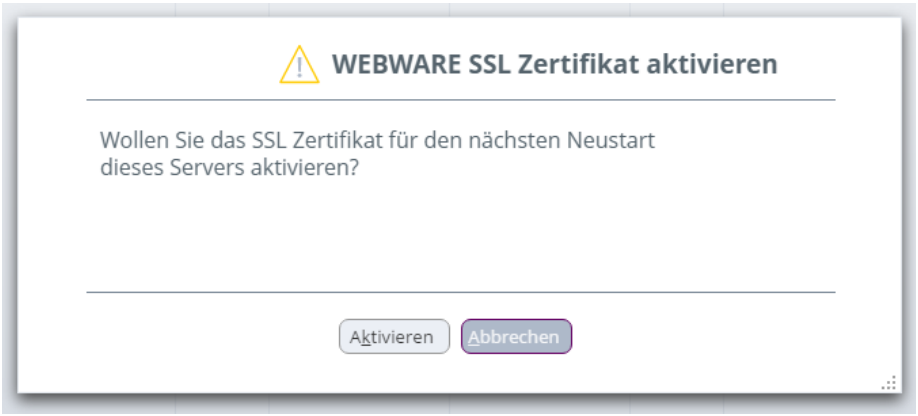
Klicken Sie hier auf Starten, so wird ein interner HTTPS-Server gestartet und in Ihrem Browser eine neue Seite mit dem Browser-Zugang angezeigt.

Der Server Beendet sich automatisch nach 1 Minute. Sie können sich zum Beispiel im Chrome-Browser mit F12 in den Entwickler-Tools (Karteikarte Security) weitere Informationen zu dem Zertifikat aufrufen.



Nach Neustart Aktivieren

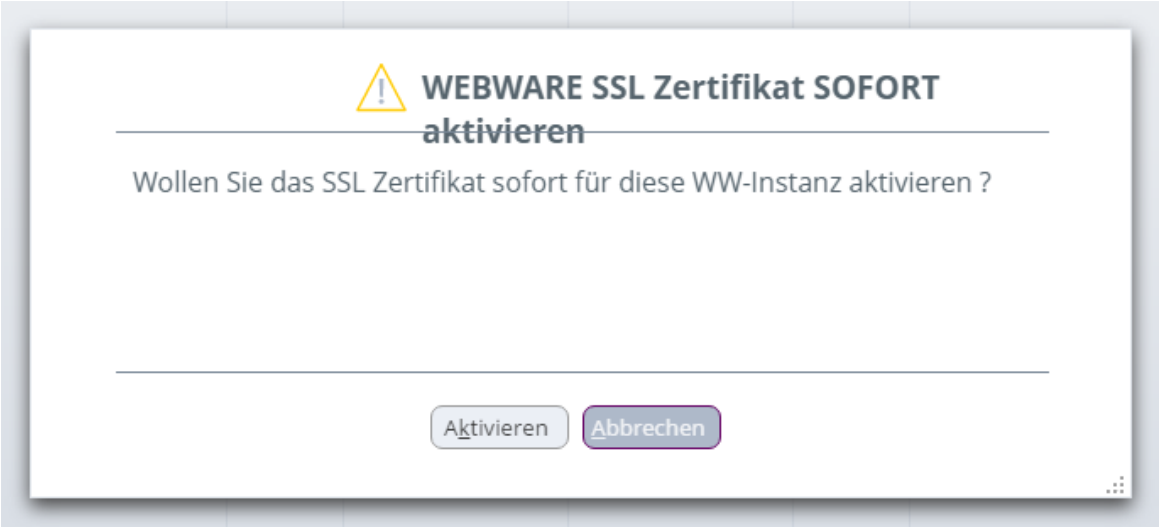
Mit dieser Funktion können Sie ein Zertifikat aus "Meine Zertifikate" als aktives Zertifikat eintragen. Dabei werden die notwendigen Informationen für das Zertifikat eingetragen, und beim nächsten Neustart der WEBWARE wird das Zertifikat dann als Standardzertifikat ausgeliefert.



Sofort Aktivieren

Mit dieser Funktion können Sie ein Zertifikat aus "Meine Zertifikate" als aktives Zertifikat eintragen. Dabei wird das Zertifikat für zukünftige Verbindungsaufbauten verwendet. Diese Funktion kann unter Umständen Seiteneffekte auslösen und sollte nur im Notfall eingesetzt werden. Im Programm entsteht dadurch ein Speicherbereich welcher nicht freigegeben wird.

Denken Sie daran das Sie bei Problemen mit dem Zertifikat keinen Zugang mehr zu Ihrem System haben. Bitte Testen Sie daher das Zertifikat mit der Funktion "Zertifikat Testen" ob es von Ihren Browsern akzeptiert wird.



Beantworten Sie den Dialog mit "Aktivieren" so wird das Zertifikat direkt eingetragen und verwendet.

Da Ihr WEBWARE System zu diesem Zeitpunkt sicherlich mehrere Verbindungen mit dem alten Zertifikat offen hat, werden diese Verbindungen beibehalten und nur neue Verbindungen mit dem neuen Zertifikat geöffnet. Dadurch kann sichergestellt werden das die bestehenden Anwendungen weiter arbeiten können.

Mit HTTP ein neues Zertifikat erstellen

Voraussetzung HTTP Challenge:

Der WEBWARE-Server muss einen HTTP-Server auf Port 80 auf dem WW-Server Rechner erstellen können und dieser HTTP-Server muss aus dem Internet unter der Zertifikatsdomain erreichbar sein.

Wenn Sie im Baum den Ast "mit HTTP neues Zertifikat erstellen" auswählen, so können Sie die Rahmenparameter vorgeben, mit denen das Zertifikat erstellt werden soll.

Folgende Parameter sind teilweise optional (o.) vorzugeben:

Kontakt eMail Let's Encrypt

Geben Sie eine gültige eMail Adresse an, welche von Let's Encrypt intern gespeichert und bei eventuellen zukünftigen Problemen für, das Zertifikat betreffende Meldungen, verwendet wird. Die Angabe einer gültigen eMail Adresse ist zwingend.

Haupt-Domain für Zertifiakt

Geben Sie hier die Haupt-Domain an, für die das Zertifikat ausgestellt werden soll. Dieses Feld ist zwingend und wird im weiteren bei der Zertifikatsprüfung von Let's Encrypt (Zertifikats-Austeller) verwendet, um auf den HTTP-Server (Port 80) der WEBWARE zuzugreifen.

Zusätzliche Sub-Domain Liste (optional)

Sie können weitere Sub-Domains angeben, die in dem zu erstellendem Zertifikat enthalten sein sollen. Werden mehrere Sub-Domains angegeben, so müssen diese mit einem Komma ohne Leerzeichen voneinander getrennt werden.

Achtung: Die Zertifikats-Prüfung wird ebenfalls für jede Sub-Domain durchgeführt. Dies bedeutet das der WW-Server, welcher den HTTP-Server für die Dateiprüfung bereit stellt, auch über die angegebenen Sub-Domains aus dem Internet ansprechbar sein muss.

Werden neben der Haupt-Domain auch Sub-Domains angegeben, so kann das Zertifikat nur erfolgreich erstellt werden, wenn alle Prüfungen der Haupt-Domain und Sub-Domains erfolgreich abgeschlossen werden. Ebenso dürfen nicht mehr als 100 Sub-Domains bei der Erstellung mitgegeben werden.

Ländercode

Geben Sie hier einen 2-stelligen Ländercode vor, der für das Zertifikat verwendet wird. Der Ländercode bezeichnet das Land in dem Ihr WW-Server System aufgestellt ist, bzw. ihre Firma angesiedelt ist.

Sie finden unter folgendem link eine Liste von möglichen Codes

https://www.digicert.com/ssl-certificate-country-codes.htm

(Bsp.: Deutschland DE, Österreich AT,..)

Firmen Namen Zertifikat (optional)

Geben Sie hier optional einen Namen für Ihre Firma an, für die dieses Zertifikat ausgestellt wird. Das Feld muss nicht zwingend ausgefüllt werden.

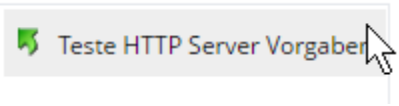
Firmen eMail Zertifikat

Geben Sie hier eine gültige eMail-Adresse die ins Zertifikat eingetragen werden soll.

HTTP Pfad Home-Verzeichnis

Wenn der HTTP-Server gestartet wird, so wird dieses Verzeichnis als HOME-Verzeichnis verwendet. Dieses Verzeichnis muss zwingend angegeben werden. Hier wird das aktuelle HOME-Verzeichnis Ihrer WEBWARE-Instanz vorgeschlagen

HTTP Netzwerkkarte (HTTP = 80)



Geben Sie hier die Netzwerkkarte an, über die der WEBWARE-Server aus dem Internet auf dem Port 80 ansprechbar ist. Hier wird die Netzwerkkarte vorgeschlagen welche für Ihre WEBWARE-Instanz verwendet wird.

HTTP abweichender Port 80

Hier können Sie einen abweichenden internen Port für die HTTP-Challenge angeben. Es ist zu Beachten das der Zugriff für die Prüfung des Zertifikats von Let's Encrypt immer über Port 80 erfolgt. Falls Sie jedoch einen Proxy/Router vorgeschaltet haben mit dem Sie den externen Port 80 auf einen anderen internen Port routen/mappen, können Sie hier den abweichenden internen Port angeben.

Bsp.: Extern http://softengine.de (Zugriff erfolgt per HTTP also Port 80). Der Router setzt den externen Port 80 auf den internen HTTP-Port 8080 für den WW-Server um. Geben Sie dann in diesem Feld den Port 8080 (intern) an

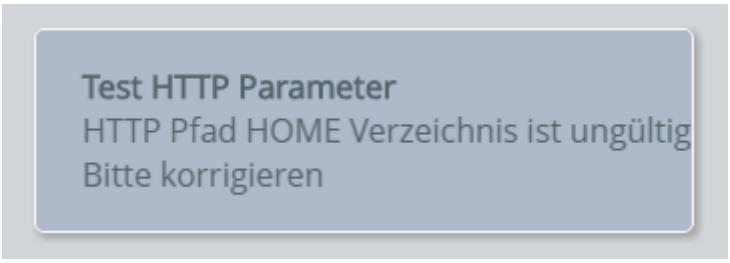
Funktion Teste HTTP Server Vorgaben

Damit Sie prüfen können, ob der WEBWARE-Server den integrierten HTTP Server Port 80 starten kann, besteht die Möglichkeit, mit der Funktion (Teste HTTP Server Vorgaben) einen Test-Server mit einer Laufzeit von einer Minute starten.

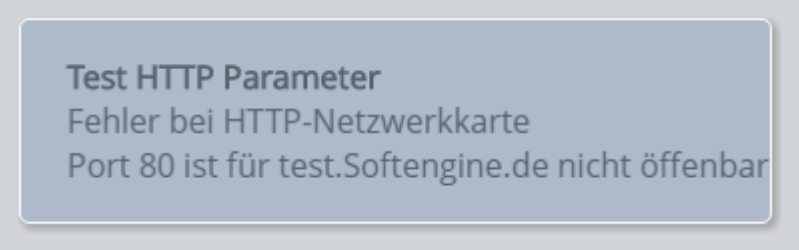
Neben dem HOME-Pfad wird auch der Parameter "HTTP-Netzwerkkarte Port 80" für den Server verwendet.

Sie erhalten dabei folgende Hinweismeldungen

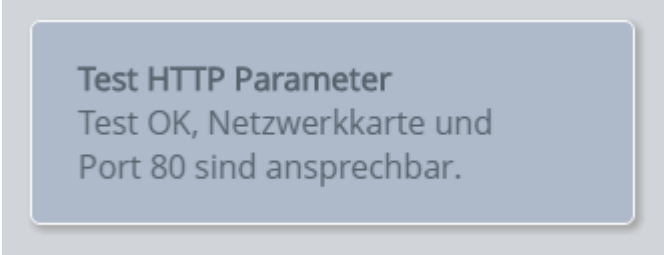
HTTP Pfad Home-Verzeichnis ist nicht vorhanden/ansprechbar

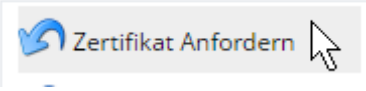


HTTP Netzwerkkarte Port 80 nicht öffenbar
Wenn die Netzwerkkarte nicht vorhanden ist bzw. der Port von einem anderen Programm blockiert ist, so erhalten Sie folgende Fehlermeldung.



OK Netzwerkkarte Port 80 ist anwendbar



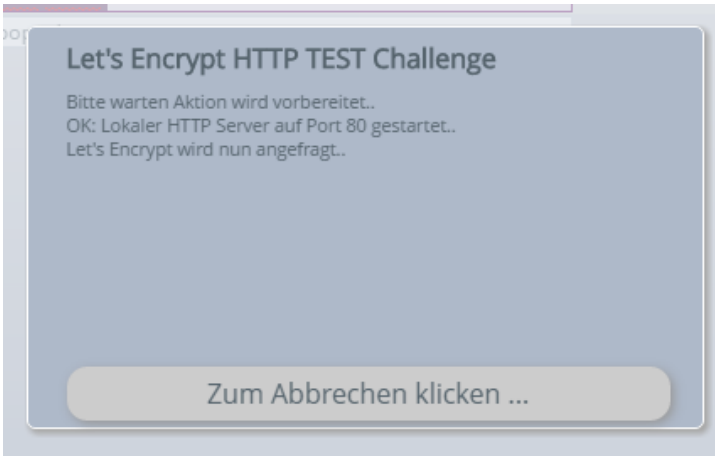


HTTP Challenge: Zertifikat Anfordern

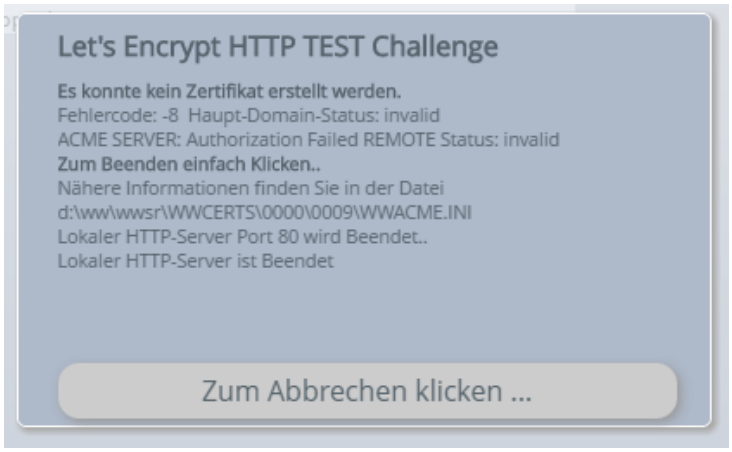
Wollen Sie ein neues Zertifikat anfordern, so können Sie das nach Angabe der Parameter mit diesem Befehl auslösen.

Bitte beachten Sie, dass die Anzahl von Zertifikaten die pro Domain erstellt werden können, beschränkt ist. Um die Ressourcen von Let's Encrypt zu schonen, sollten Sie für Test's und Prüfung der Eingabeparameter die Funktion "Test-Zertifikat Anfordern" verwenden, da hier kein Beschränkung gilt und das Zertifikat nicht global gültig ist.

Nach Auslösen von „Zertifikat Anfordern“ werden die Zertifikats-Informationen zusammengestellt und eine Konfigurationsdatei erstellt. Ebenso wird für die Dauer der Zertifikatsprüfung der integrierte HTTP Port 80 Server gestartet. Dann wird das Programm bin\wws\wwcers\bin\wwacme.exe gestartet, welches die Zertifikatserstellung übernimmt.
Sie erhalten mit Hilfe eines Hinweis-Fenster Informationen über den Fortschritt.



Je nach Erfolg oder Misserfolg erhalten Sie dann eine Hinweismeldung.



Konnte ein Zertifikat erstellt werden, so wird dieses in der Zertifikats-Liste im Bereich "Meine Zertifikate" angezeigt und Sie können es von dort aus Aktivieren.

HTTP Challenge: Test-Zertifikat anfordern

Um die Ressourcen von Let's Encrypt zu schonen, sollten Sie immer erst versuchen ein Test-Zertifikat zu erstellen. Das hat den Nachteil das es nicht als gültiges Zertifikat eingesetzt werden kann, die Test-Zertifikate aber nicht in der Menge begrenzt sind.

Ansonsten ist der Ablauf gleich zu der normalen Zertifikat Erstellung.

Mit FTP ein neues Zertifikat erstellen

Voraussetzung FTP Challenge:

Der WEBWARE-Server baut während der Dateiprüfung für das Zertifikat eine Verbindung zu Ihrem FTP-Server auf und überträgt in ein Verzeichnis eine Datei, welche vom Let's Encrypt Dienst dort abgerufen wird. Daher werden für diesen Vorgang die Zugangsdaten zu dem FTP-Server der Domain benötigt für den das Zertifikat erstellt wird.

Bei der FTP-Challenge werden Verzeichnisse und Dateien per FTP auf den Server geschrieben welcher per HTTP Port 80 für die Domain Daten ausliefert. Die Verzeichnisse und Dateien werden nach der Prüfung wieder gelöscht.

FTP Challenge:

Folgende Parameter sind teilweise optional (o.) vorzugeben.

Kontakt eMail Let's Encrypt

Geben Sie eine gültige eMail Adresse an welche von Let's Encrypt intern gespeichert wird, und bei Problemen in der Zukunft für Meldungen das Zertifikat betreffend verwendet wird. Die Angabe einer gültigen eMail Adresse ist zwingend.

Haupt-Domain für Zertifikat

Geben Sie hier die Haupt-Domain an für welche das Zertifikat ausgestellt werden soll. Diese Feld ist zwingend und wird im weiteren bei der Zertifikatsprüfung von Let's Encrypt (Zertifikat-Austeller) verwendet, um auf den HTTP-Server (Port 80) der WEBWARE zuzugreifen.

zusätzliche Sub-Domain Liste (optional)

Sie können weitere Sub-Domains angeben welche in dem zu erstellendem Zertifikat enthalten sein sollen. Werden mehrere Sub-Domains angegeben so müssen diese mit einem Komma ohne Leerzeichen von- einander getrennt werden.

Achtung: Die Zertifikats-Prüfung wird ebenfalls für jede Sub-Domain durchgeführt. Dies bedeutet das der WW-Server welcher den HTTP-Server für die Dateiprüfung bereit stellt auch über die angegebenen Sub-Domains aus dem Internet ansprechbar sein muss.

Werden neben der Haupt-Domain, Sub-Domains angegeben so kann das Zertifikat nur erfolgreich erstellt werden wenn alle Prüfungen der Haupt-Domain und Sub-Domains erfolgreich abgeschlossen werden. Ebenso dürfen nicht mehr als 100 Sub-Domains bei der Erstellung mitgegeben werden.

Ländercode

Geben Sie hier einen 2-stelligen Ländercode vor, der für das Zertifikat verwendet wird. Der Ländercode bezeichnet das Land in dem Ihr WW-Server System aufgestellt ist, bzw. ihre Firma angesiedelt ist.

Sie finden unter folgendem link eine Liste von möglichen Codes

https://www.digicert.com/ssl-certificate-country-codes.htm

(Bsp.: Deutschland DE, Österreich AT,..)

Firmen Namen Zertifikat (optional)

Geben Sie hier optional einen Namen für Ihre Firma an für die dieses Zertifikat ausgestellt wird. Das Feld muss nicht zwingend ausgefüllt werden.

Firmen eMail Zertifikat

Geben Sie hier eine gültige eMail-Adresse die ins Zertifikat eingetargen werden soll.

FTP Serveradresse

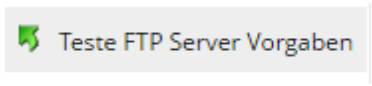
Geben Sie hier die FTP-Serveradresse des FTP-Servers an, welcher die HTTP-Dateien für die Domain-Adresse ausliefert. Die FTP-Adresse muss mit ftp:// beginnen. Hier wurde am 20.05.2017 eine Korrektur vorgenommen, da bisher immer ein / am Ende der Adresse erwartet wurde. Diese wird nun intern automatisch angefügt.

FTP Benutzername

Geben Sie hier den Benutzer für den FTP-Server an, mit dem Dateien und Verzeichnisse in das Root-Verzeichnis der Domain geschrieben werden können.

FTP Passwort

Geben Sie hier das Passwort an, welches für den Zugang zu dem FTP Server benötigt wird. Das FTP-Passwort wird in eine INI-Datei geschrieben und nach der Durchführung



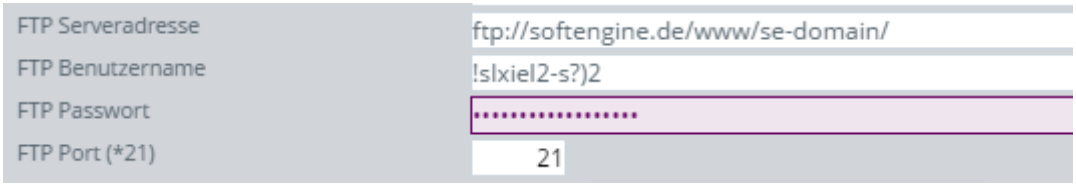
unkenntlich gemacht. Sie haben die Möglichkeit, das Passwort (per Default) mit dem System-Wert (Vorgabewerte für Zertifikate > FTP-Passwort speichern) auch in der WEBWARE internen Datenbank verschlüsselt abzulegen, so dass es bei erneutem Zugriff automatisch vorgeschlagen wird.

FTP-Port

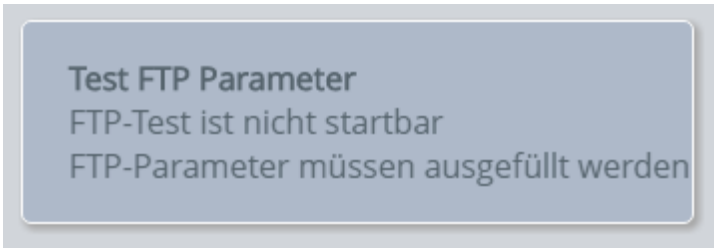
Hier wird der Standardport 21 vorgegeben.

Funktion Teste FTP Server Vorgaben

Mit dieser Funktion können Sie die Zugangsdaten für einen FTP-Server testen. Dabei wird eine Verbindung zum Test-Server aufgebaut, ein Verzeichnis und eine Datei angelegt und gleich wieder gelöscht. Sie benötigen dabei folgende Vorgabewerte:

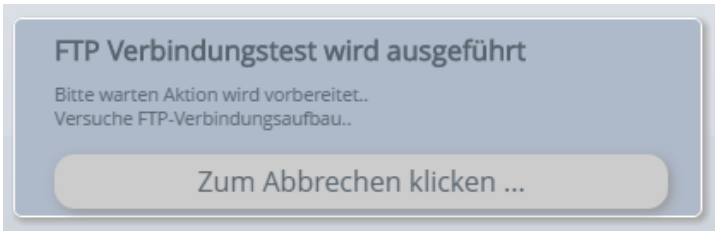


Sind die FTP-Parameter nicht vollständig ausgefüllt so erhalten Sie eine Fehlermeldung:

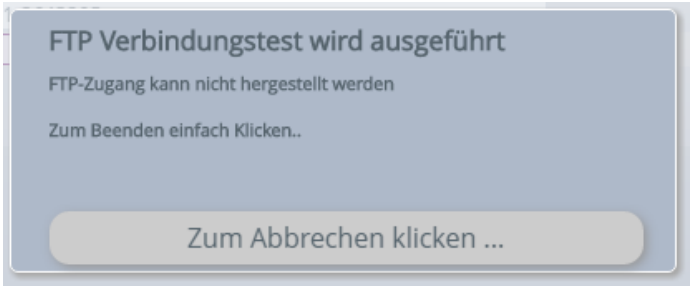


Sind die Parameter vorhanden, so wird eine Hinweisdialog mit dem Fortschritt angezeigt.

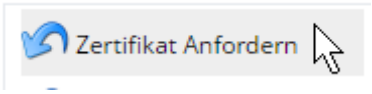
Zuerst der Start der Verbindung:



Gibt es beim Zugriff Probleme erhalten Sie folgenden Hinweis:



Nach erfolgreichem Zugriff erhalten Sie eine Erfolgsmeldung:



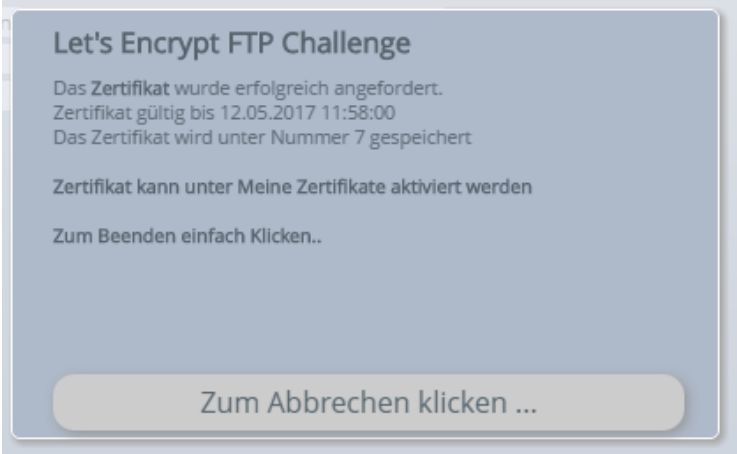
FTP Challenge: Zertifikat Anfordern

Wollen Sie ein neues Zertifikat anfordern, so können Sie das, nach Angabe der Parameter, mit diesem Befehl auslösen.

Bitte beachten Sie, dass die Anzahl von Zertifikaten die pro Domain erstellt werden können, beschränkt ist. Um die Ressourcen von Let's Encrypt zu schonen, sollten Sie für Test's und Prüfung der Eingabeparameter die Funktion "Test-Zertifikat Anfordern" verwenden da hier kein Beschränkung gilt und das Zertifikat nicht global gültig ist.

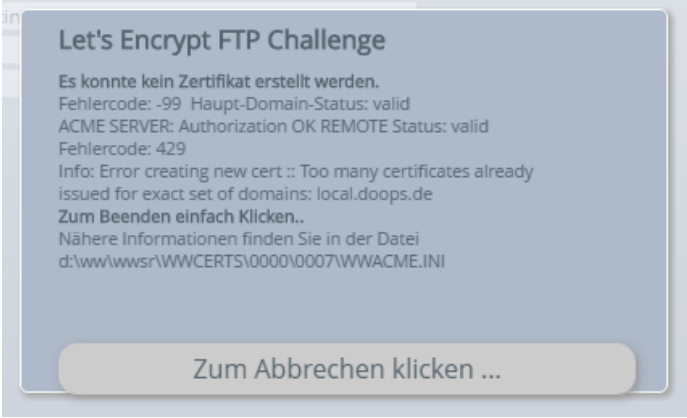
Nach dem Auslösen von „Zertifikat Anfordern“, werden die Zertifikats-Informationen zusammengestellt und eine Konfigurationsdatei erstellt.
Dann wird das Programm bin\wws\wwcers\bin\wwacme.exe gestartet, welches die Zertifikatserstellung übernimmt.
Sie erhalten mit Hilfe eines Hinweis-Fenster Informationen über den Fortschritt.

Je nach Erfolg oder Misserfolg erhalten Sie dann eine Hinweismeldung.



Konnte ein Zertifikat erstellt werden, so wird dieses in der Zertifikats-Liste im Bereich "Meine Zertifikate" angezeigt und Sie können es von dort aus Aktivieren.

Tritt ein Fehler auf so erhält man nähere Informationen aus der Hinweismeldung.

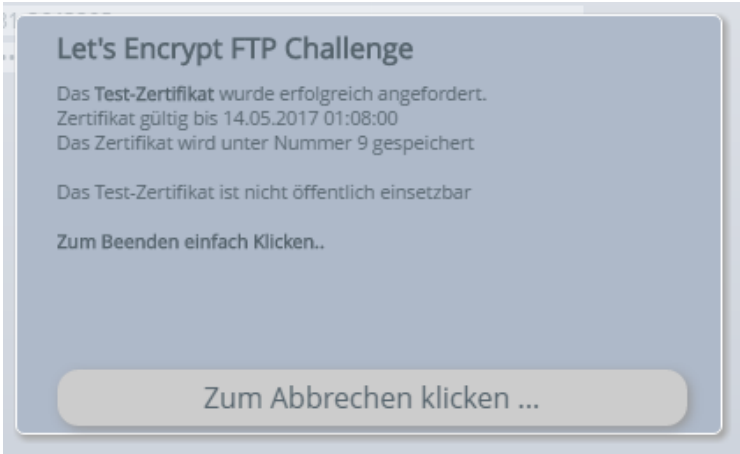


Weitere Informationen, gerade bei Benutzung von SUB-Domains findet man auch in der INI-Datei im angegebenen Pfad.

FTP Challenge: Test-Zertifikat anfordern

Um die Ressourcen von Let's Encrypt zu schonen sollten Sie immer erst versuchen ein Test-Zertifikat zu Erstellen. Dieses hat den Nachteil das es nicht als gültiges Zertifikat eingesetzt werden kann, die Test-Zertifikate aber nicht in der Menge begrenzt sind.

Ansonsten ist der Ablauf gleich zu der normalen Zertifikat Erstellung.



Verwaltung der Zertifikate

Die Zertifikate werden in folgender Hierarchie im Verzeichnis
bin\wws\wwcerts
abgespeichert.

bin\wws\wwcerts\[4-Stellige WW-Instanz-ID]\[4-Stellige laufende Nummer des Zertifikats]

Ein Verzeichnis bzw. die Konfigurations-Datei sieht dann so aus

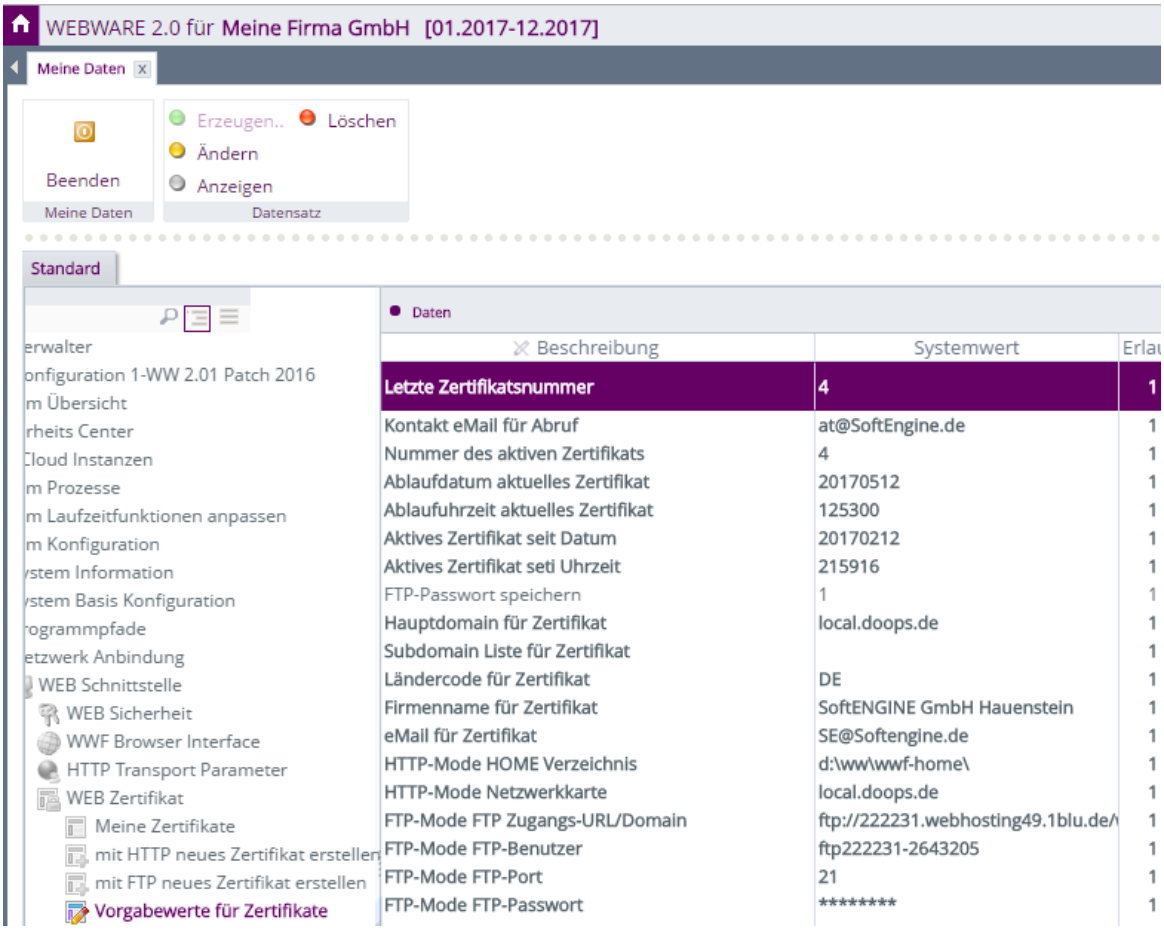
bin\wws\wwcerts\0000\0003\wwacme.ini

Bei einem gültigen Zertifikat finden Sie unterhalb des Zertifikatsordners im Ordner CERTS die 4 WW-Zertifikatsdateien.

Im Ordner CERTS\ORIGINAL finden Sie alle Dateien die von Let's Encrypt erstellt wurden.

Vorgabewerte für Zertifikate

Sie finden hier alle Parameter die für die Zertifikatsverwaltung benötigt werden. Die meisten Parameter werden zur Vereinfachung direkt aus den Eingabemasken der Zertifikatserstellung übernommen und gespeichert.



Hier die einzelnen Parameter in der Übersicht:

Letzte Zertifikatsnummer:	Letzte Nummer die für Zertifikate vergeben wurde
Kontakt eMail für Abruf	eMail-Adresse die für Let's Encrpyt verwendet wird
Nummer des aktiven Zertifikats	Nummer des aktiven Zertifikats
Ablaufdatum aktuelles Zertifikat	Wie lange ist das aktuelle Zertifikat gültig
Ablaufuhrzeit aktuelles Zertifikat	Bis zu welcher Uhrzeit ist das Zertifikat gültig
Aktives Zertifikat seit Datum	Wann wurde das Zertifikat als Aktives eingetragen
Aktives Zertifikat seit Uhrzeit	Wann wurde das Zertifikat als Aktives eingetragen
FTP-Passwort speichern	Soll das FTP-Passwort in der WW gespeichert werden ?

Die weiteren Parameter sind Sicherungen der Eingabe aus den Zertifikats-Dialogen..

Fehlermeldungen/Fehlercodes von WWACME.EXE

Fehlercode	Grund
1	OK Zertifikatsanfrage war erfolgreich
-1	INTERN: Kein Konfigurationspfad angegeben (Es fehlt CONFIG Eintrag in INI)
-2	INTERN Kein Zielpfad für Zertifikate angegeben (WWACME_CERT_PATH)
-3	INTERN: Keine eMail Adresse angegeben (WWACME_EMAIL)
-4	INTERN: Keine Domain angegeben (WWACME_DOMAIN/DOMAIN)
-5	INTERN: Kein HOME-Pfad für HTTP Challenge angegeben (WWACME_HTTP_HOMEDIR/CONFIG
-8	Fehler bei Validierung. Der Entfernte Server konnte nicht auf Ihr HOME-Verzeichnis zugreifen, bzw. die Validierung ist fehlgeschlagen. Nähere Informationen untern bin\wws\wwcerts\bin\logs
-10	INTERN: Keine FTP Ziel-Domain für FTP Challenge angegeben (WWACME_FTP_DOMAIN/CONFIG)
-11	INTERN: Kein FTP Benutzernamen für FTP Challenge angegeben (WWACME_FTP_USER/CONFIG)
-12	INTERN: Kein FTP Passwort für FTP Challenge angegeben (WWACME_FTP_PASSWORD/CONFIG)
-99	Fehler Ausnahme im Programm aufgetreten nähere Infos unter bin\wwcerts\bin\logs

Änderungen an diesem Dokument

Datum	Version	Änderung
17.09.2013	1.0	Start dieses Dokumentes
03.06.2015	1.01	Erweiterung
29.06.2015	1.02	Erweiterung
02.07.2015	1.03	Erweiterung
13.02.2017	2.0	Erweiterung Let's Encrypt
16.02.2017	2.01	Finalize Dokumentation Let's Enrypt
20.02.2017	2.02	Erweiterung Port 80 bei HTTP Challenge änderbar
16.07.2017	2.03	Zertifikat meine-webware.de nun von Let's Encrypt erstellt. Gültig bis 13.10.2017
04.09.2017	2.04	Zertifikat meine-webware.de wurde erneuert und ist nun Gültig bis 03.12.2017