TOPAL ZERTIFIKAT MANAGER

ANLEITUNG ZUR ERSTELLUNG VON ZERTIFIKATEN

Version	Date	Author	Status	Comment
0.1	21.09.2014	Hunkeler Bruno	In work	Initial Version
1.0	12.11.2014	Hunkeler Bruno	Final	Final Version

Table of content

1. Management Summary 4
1.1 Übersicht 4

2. Installation und Konfiguration des Zertifikatsmanagers 4
2.1 Directory Struktur 4
2.2 Konfiguration Ihres Rechners: 6
2.3 Anpassung des Batch Files zur Erstellung von Zertifikaten für einen Kunden 10
2.4 Erstellen von Zertifikaten für einen Kunden 12
2.4.1 Ausstellen eines Self Signed Root Zertifikats 12
2.4.2 Ausstellen von Server Zertifikaten 14
2.4.3 Ausstellen von User Zertifikaten 15

3. Anhang 16
3.1 Glossar / Definitionen, Akronym und Abkürzungen 16

Abbildungsverzeichnis

Figure 1 Certificate Manager Directory....4
Figure 2 MakeCert Directory....5
Abbildung 3 Erweiterte Systemeinstellungen....6
Abbildung 4 Umgebungsvariablen....7
Abbildung 5 Systemvariabeln....7
Abbildung 6 Neue Systemvariabel erstellen....8
Abbildung 7 Einfügen der neuen Systemvariablen....8
Abbildung 8 Systempfadanpassung....9
Abbildung 9 Systempfad Verifikation....9
Abbildung 10 Zertifikatskette....12
Abbildung 11 Rootzertifikat erstellen....13
Abbildung 12 Passwortverifikation....13
Abbildung 13 Serverzertifikat erstellen....14
Abbildung 14 Passwortverifikation bei Serverzertifikat....14
Abbildung 15 Userzertifikat erstellen....15
Abbildung 16 Passwortverifikation bei Userzertifikat....15

Tabellenverzeichnis

Tabelle 1 Glossar / Definitionen, Akronym und Abkürzungen....16

1. MANAGEMENT SUMMARY

1.1 Übersicht

Mit der Version V7.6.3.0 von Topal wird die Kommunikation via SSL bereitgestellt. Die Erstellung von Zertifikaten kann als Service für Topal Vertriebspartner gesehen werden. Bei der momentan verfügbaren Applikation (Batch File) handelt es sich um eine „Commandline" Applikation.

2. INSTALLATION UND KONFIGURATION DES ZERTIFIKATSMANAGERS

Die momentan Verfügbare Version wird steht den Vertriebspartnern unter folgendem Link zur Verfügung:

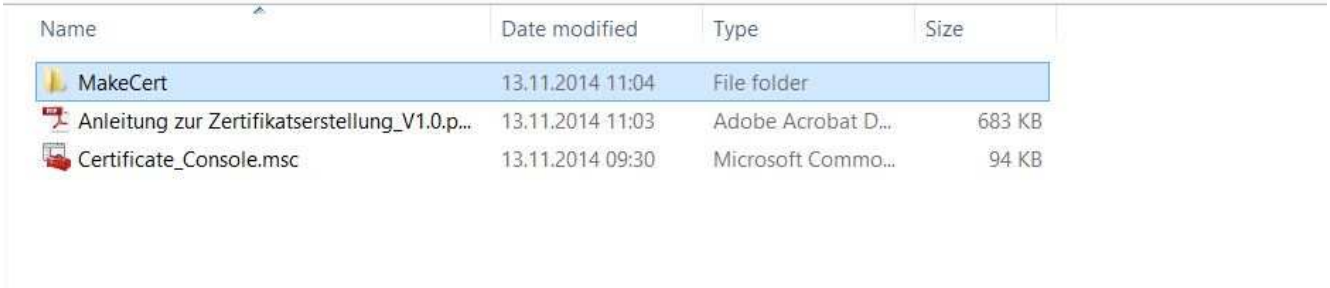
Downloadlink

Laden Sie das Zip File vom angegebenen FTP Server und entzippen Sie dieses an die gewünschte Stelle. Das entzippte Directory beinhaltet alle notwendigen Libraries zur Erstellung von „Self Signed Zertifikaten".

2.1 Directory Struktur

Im Directory **Certificate_Manager** finden Sie die folgenden Struktur.

MakeCert	Beinhaltet Dateien zur Erstellung von
Certificate_Console.msc	Aufrufen des Zertifikatsmanagers
Anleitung zur Zertifikatserstellung.pdf	Anleitung



Name	Date modified	Type	Size
MakeCert	13.11.2014 11:04	File folder	
Anleitung zur Zertifikatserstellung_V1.0.p...	13.11.2014 11:03	Adobe Acrobat D...	683 KB
Certificate_Console.msc	13.11.2014 09:30	Microsoft Commo...	94 KB

Figure 1 Certificate Manager Directory

Im Directory **MakeCert** finden Sie die folgenden Dateien.

Name	Date modified	Type	Size
_install.bat	13.11.2014 09:30	Windows Batch File	3 KB
_uninstall.bat	13.11.2014 09:30	Windows Batch File	2 KB
capicom.dll	13.11.2014 09:30	Application extens...	500 KB
Certificate_Console.msc	13.11.2014 10:57	Microsoft Commo...	93 KB
CStore.vbs	13.11.2014 09:30	VBScript Script File	76 KB
makecert.exe	13.11.2014 09:30	Application	55 KB
pvk2pfx.exe	13.11.2014 09:30	Application	25 KB
readme.txt	13.11.2014 09:30	Text Document	1 KB
TopalCertificate_Walser.bat	13.11.2014 10:56	Windows Batch File	2 KB

Figure 2 MakeCert Directory

Es handelt sich bei diesen Dateien um Libraries und Batchdateien zur Erstellung von Zertifikaten. Die Relevante Datei zur Erstellung von Zertifikaten ist die **TopalCertificate_Walser.bat** mit dieser Datei werden Root-, Server- und Benutzerzertifikate erstellt.

Die Batchdatei **TopalCertificate_Walser.bat** ist ein Beispiel, wie das Batchfile für die Erstellung von Zertifikaten für einen 3. Kunden konfiguriert werden muss.

Die einzelnen Schritte werden in den folgenden Kapiteln beschrieben.

2.2 Konfiguration Ihres Rechners:

Damit Ihr Computer die gewünschten Dateien des Certicate_Managers findet, sind die entsprechenden Dateien (Libraries) im System Pfad zu konfigurieren:

Dies wird in folgenden Schritten beschrieben:

1. Öffnen Sie System Einstellungen via
   [Start | Systemsteuerung | System und Sicherheit | System] in der Menünavigation (Menü Links) finden Sie den Link **[Erweiterte Systemeinstellungen]**.

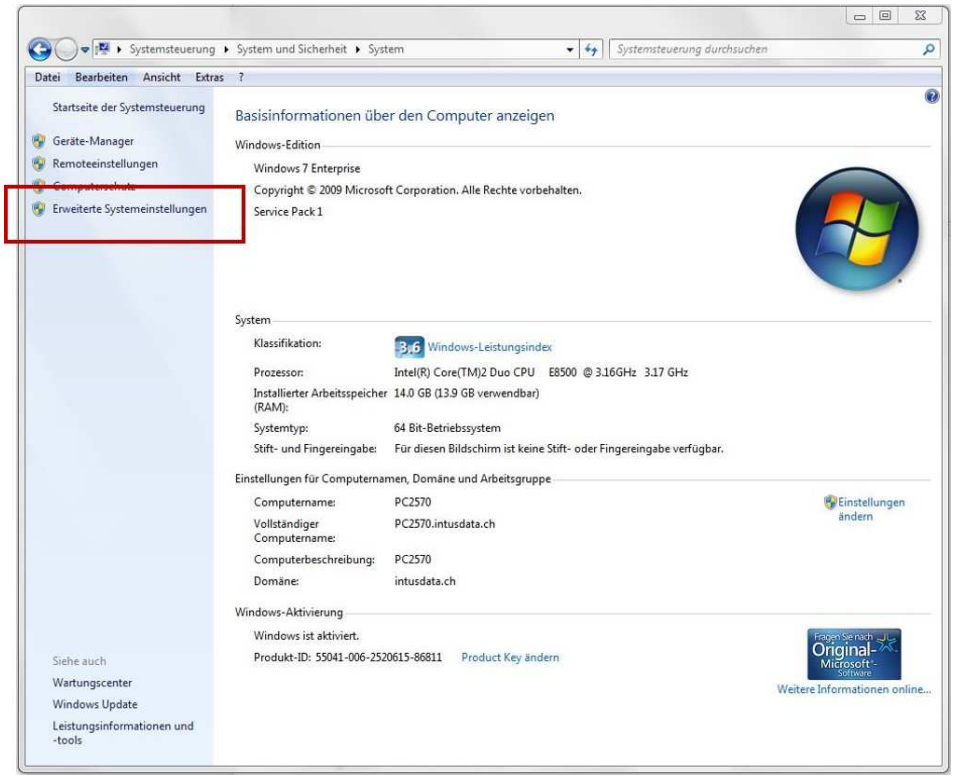


Abbildung 3 Erweiterte Systemeinstellungen

2. Definieren der Umgebungsvariablen.
   Nach dem Anwählen des Links **[Erweiterte Systemeinstellungen]** wird der nachfolgende Dialog geöffnet. Wählen Sie den Button **[Umgebungsvariabeln]**

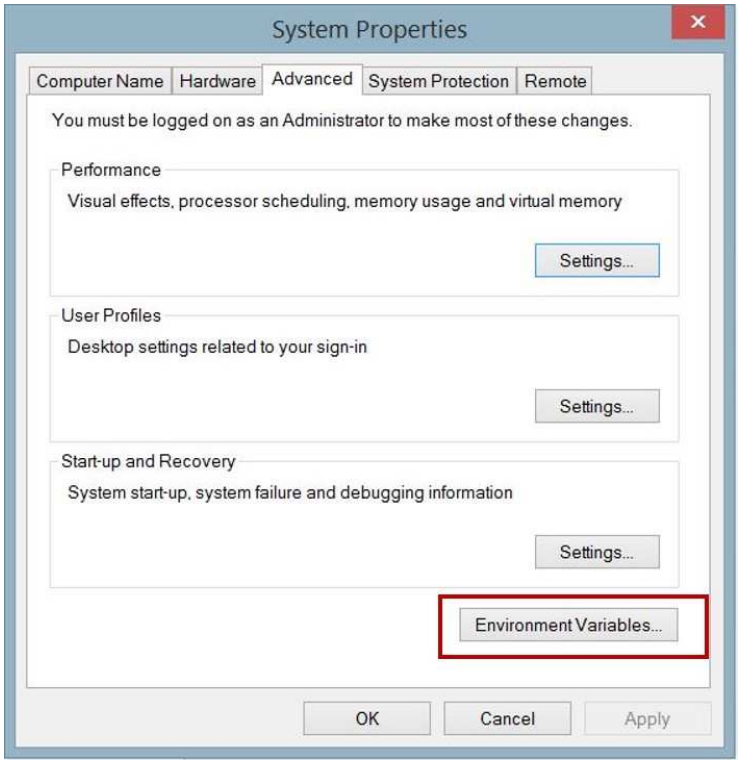


Abbildung 4 Umgebungsvariablen

Nachdem Sie den Button gewählt haben, wir der Dialog in Abschnitt 3 ersichtlich.

3. Setzen der Umgebungsvariablen (Systemvariabeln).
   Damit Ihr System den Certificate_Creator findet, ist es notwendig Ihrem System diesen Pfad bekannt zu machen. Dies erreichen Sie indem Sie die nachfolgenden Schritte durchführen.

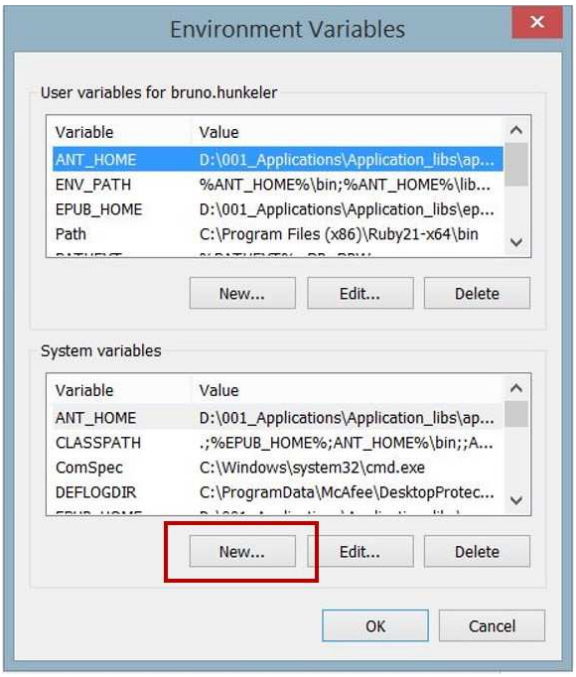


Abbildung 5 Systemvariabeln

4. Erstellen Sie eine neue Systemvariable:
   Wählen Sie den Button **[Neu]** im Bereich **Systemvariabeln**. Der nachfolgende Dialog wird geöffnet:

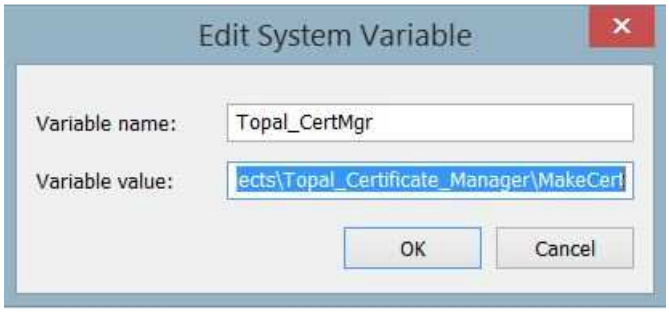


Abbildung 6 Neue Systemvariabel erstellen

Name der Variablen: z:B **Topal_CertMgr**
Wert der Variablen: Pfad an dem Sie den „Certificate Manager" abgelegt haben.

Hierbei ist es wichtig, dass Sie den gesamten Pfad inkl. MakeCert angeben:
z.B. E:\005_Data\010_Subjects\Topal_Certificate_Manager\MakeCert

Quittieren Sie die Eingabe mit **[OK].**

5. Hinzufügen der Systemvariablen zum Systempfad
   Fügen Sie nun die neu erstellte Systemvariabel dem Systempfad hinzu.
   Hierfür suchen Sie im Grid Systemvariablen den Eintrag **[Pfad]** (siehe Abbildung).

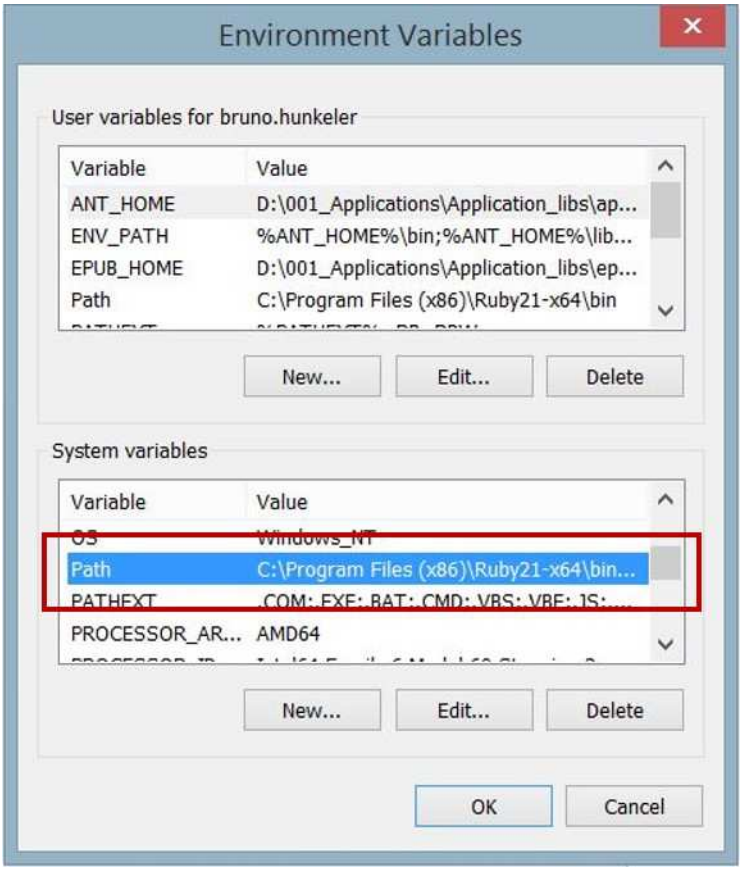


Abbildung 7 Einfügen der neuen Systemvariablen

Der nachfolgende Dialog wir geöffnet:

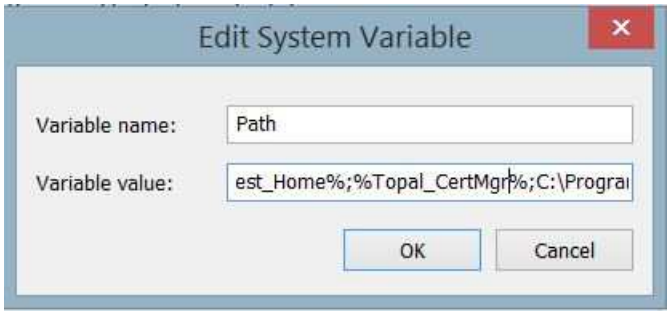


Abbildung 8 Systempfadanpassung

Fügen Sie am **Schluss** der angezeigten Zeile **[Wert der Variablen]** die folgenden Angaben hinzu:

;%Topal_CertMgr% (es ist wichtig, dass Sie das Trennzeichen „Strichpunkt" einfügen)

6. Verifizieren des Systempfades:
   Öffnen Sie die Consolen Applikation und geben Sie den Befehl **[path]** ein.

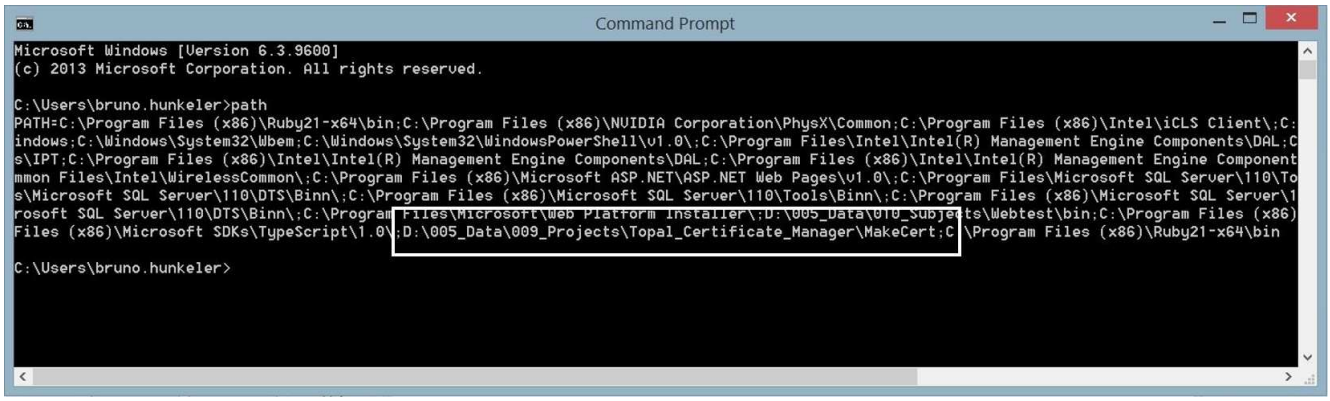


Abbildung 9 Systempfad Verifikation

Ihr neu hinzugefügter Systempfad sollte nun ersichtlich sein.

2.3 Anpassung des Batch Files zur Erstellung von Zertifikaten für einen Kunden

Ändern Sie das Batchfile wie folgt ab, um ein Root Zertifikat für einen Kunden zu erstellen. Die rot eingefärbten Bezeichnungen sind dem Namen des Rootzertifikats des Kunden anzupassen.

Bsp. Treuhand Walser CA

Pfad Anpassung: Passen Sie diesen Pfad entsprechend der Lokation des Zertifikatsordners:

```
ECHO OFF
CLS

SET CERTYPE=0
SET /p CERTYPE=Input certificate type (0: CA, 1: Client, 2: Server):
SET SKY=-sky signature

set CommonName=Treuhand Walser CA
set Quoted_CommonName="%CommonName%"


IF %CERTYPE% equ 0 (
  SET CN=%CommonName%
  SET SKY=-sky signature -ss root -sr localmachine –r
) ELSE IF %CERTYPE% equ 1 (

  SET CN=Topal Client
  SET SKY=-sky exchange -eku 1.3.6.1.5.5.7.3.2 -in %Quoted_CommonName% -is Root -ir
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12
) ELSE IF %CERTYPE% equ 2 (

  SET CN=Topal Server
  SET SKY=-sky exchange -eku 1.3.6.1.5.5.7.3.1 -in %Quoted_CommonName% -is Root -ir
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12
) ELSE (

  ECHO ERROR CERTYPE
  PAUSE
  EXIT
)

SET /p CN=Input CN of certificate (default: %CN%):
SET PASS=pass
SET /p PASS=Input certificate password (default: %PASS%):
SET CERT="CN=%CN%"
SET CNKEY="%~dp0%CN%.key"
SET CNCER="%~dp0%CN%.cer"
SET CNP12="%~dp0%CN%.p12"

IF EXIST %CNKEY% DEL /F /Q  %CNKEY%
IF EXIST %CNCER% DEL /F /Q  %CNCER%
IF EXIST %CNP12% DEL /F /Q  %CNP12%
```

```
rem ==========================================================================================
rem create a Certificate with defined algorithm, start- and end date
rem ==========================================================================================

rem change the encryption algorithm depending on your needs
rem The following algorithms can be used md5, sha1, sha256, sha384, or sha512


%MAKECERT% -pe -n %CERT% -a sha256 -b 01/01/2014 -e 01/01/2017 %SKY% -sv %CNKEY% %CNCER%


%PVK2PFX% -pvk %CNKEY% -pi "%PASS%" -spc %CNCER% -pfx %CNP12% -po "%PASS%" –f
%CERTUTIL% -f -p %PASS% -importpfx %CNP12%

PAUSE
EXIT
```

2.4 Erstellen von Zertifikaten für einen Kunden

Wie oben erwähnt besteht die Möglichkeit „Self Signed Certificates" zu verwenden respektive auszustellen. Dies kann mit dem mitgelieferten Werkzeug von Topal erreicht werden.

Folgender Sachverhalt ist wichtig bei der Erstellung von Zertifikaten. Werden verschiedene Zertifikate (Root-, Server und Userzertifikate) für einen Kunden ausgestellt haben diese eine Abhängigkeit.

Diese wird in der nachfolgenden Abbildung gezeigt. Entsprechend ist es notwendig, dass die Passwörter bei der Erstellung eines Root Zertifikats bei der Erstellung eines Server Zertifikats bekannt sein muss. Dasselbe gilt bei der Erstellung eines Userzertifikats. Dieser Sachverhalt wird in den folgenden Kapiteln nochmals beschrieben.

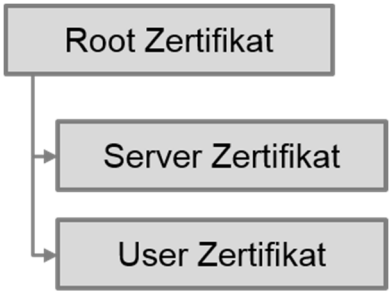


Abbildung 10 Zertifikatskette

2.4.1 Ausstellen eines Self Signed Root Zertifikats

Das mitgelieferte Werkzeug nutzt die von Windows bereitgestellten Services zur Erstellung von Self Signed Certificates. Das Werkzeug ist als Batchdatei aufgebaut.

Zur Erstellung von Zertifikaten ist wie folgt vorzugehen:

Starten Sie die Datei **TopalCertificate_Walser.bat**. Nach dem starten des Batchfiles haben Sie die Möglichkeit zur Unterscheidung zwischen verschiedenen Typen von Zertifikaten.

- 0 - CA: Dient der Erstellung eines Root Zertifikats
- 1 - Server: Dient der Erstellung von Server Zertifikaten
- 2 - Client (User): Dient der Erstellung von Benutzer Zertifikaten

Wählen Sie die 0 für CA (Certificate Authority), sowie den Namen ihrer Firma (Treuhand Walser CA) und das Passwort ein. Sind die Eingaben erfolgt, wird nach den Passwörtern zur Verschlüsselung und zur Verifikation gefragt. Geben Sie diese bitte ein. Ist dieser Schritt abgeschlossen wird das Zertifikat erzeugt und direkt im Certificate Store (Zertifikatsmanager) auf Ihrem Rechner installiert.

Bemerkung:

Beim starten der Console ist es wichtig diese als Administrator auszuführen.

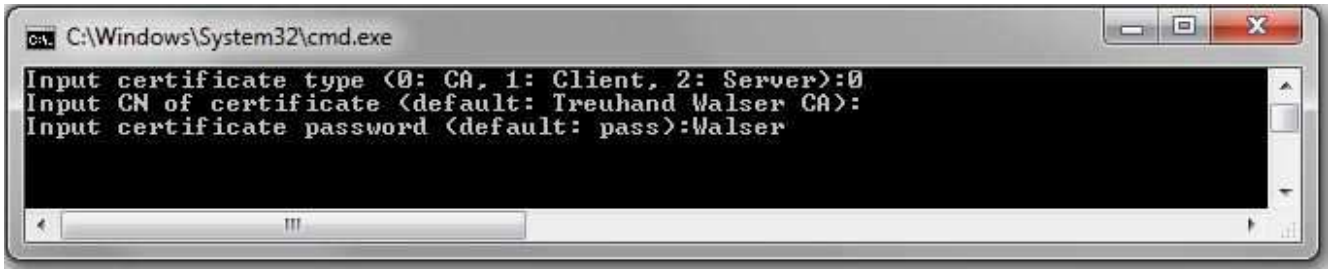


Abbildung 11 Rootzertifikat erstellen

Bei der Erstellung der Zertifikate wird eine Passwortprüfung vollzogen.

Abbildung 12 Passwortverifikation

Im Falle der Erstellung von Root Zertifikaten ist in jedem der oben gezeigten Dialogen das eingegebene Passwort zu verwenden.

2.4.2 Ausstellen von Server Zertifikaten

Die Erstellung von Serverzertifikaten wird in derselben Weise wie die oben erwähnten Root Zertifikate erstellt.

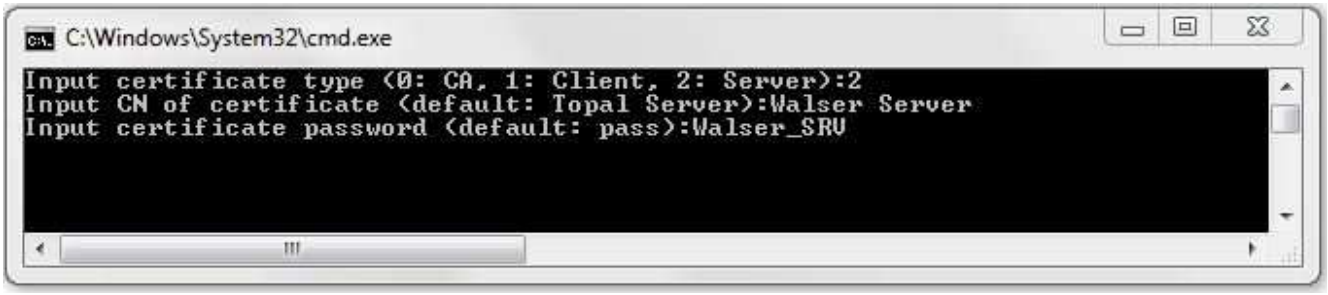


Abbildung 13 Serverzertifikat erstellen

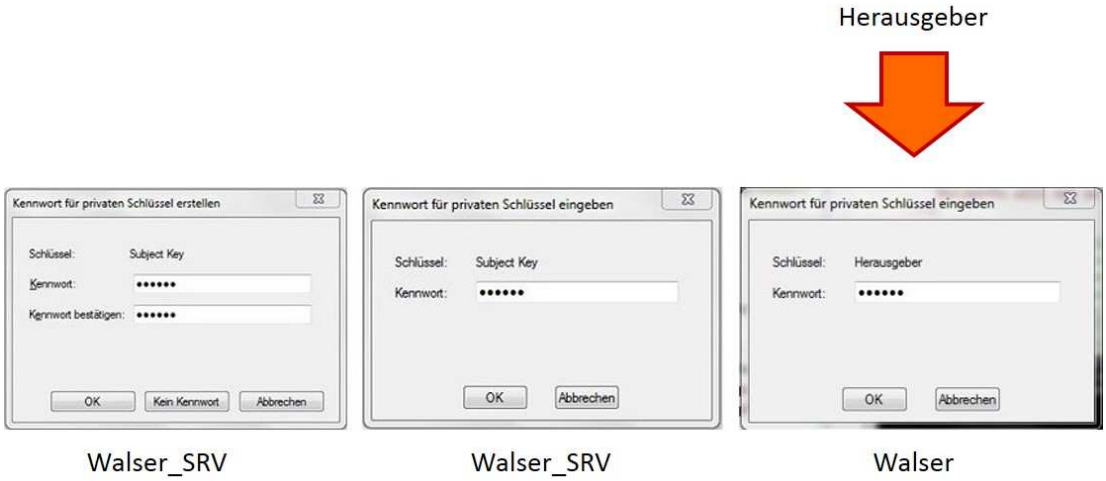


Abbildung 14 Passwortverifikation bei Serverzertifikat

Die Eingabe der Passwörter erfolgt gemäss der Abbildung 12.

2.4.3 Ausstellen von User Zertifikaten

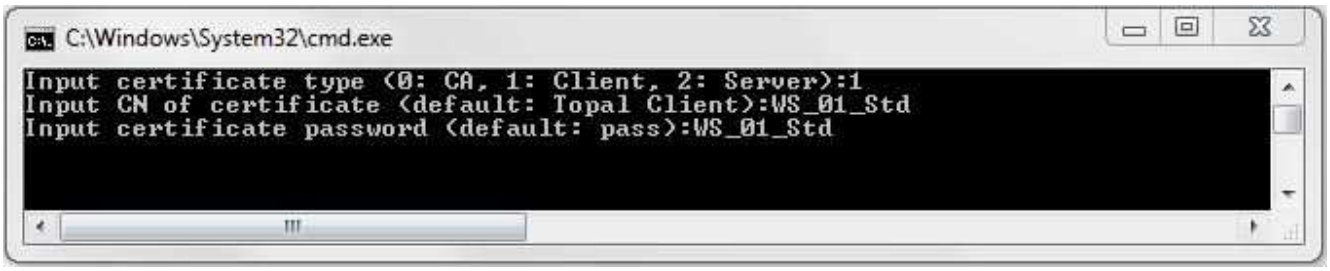


Abbildung 15 Userzertifikat erstellen

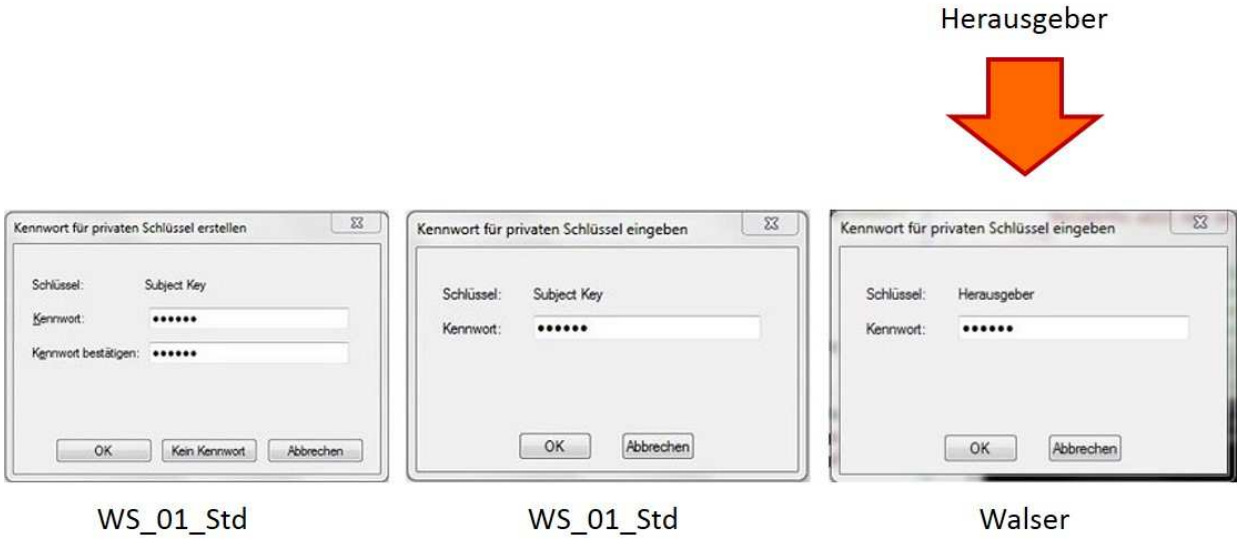


Abbildung 16 Passwortverifikation bei Userzertifikat

Die Eingabe der Passwörter erfolgt gemäss der Abbildung 13.

3. ANHANG

3.1 Glossar / Definitionen, Akronym und Abkürzungen

Term	Definition
Zertifikat	▪ Ein Zertifikat ist ein "Ausweis" im Internet. Das Zertifikat enthält Informationen über die Identität einer Person und Signaturprüfdaten, mit deren Hilfe Signaturen dieser Person zugeordnet werden können. Das Zertifikat ist durch die elektronische Signatur seines Ausstellers vor Veränderungen geschützt. ▪ Beinhaltet den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Gültigkeitsdauer sowie den Namen der Zertifizierungsstelle (engl. Certificate Authority oder kurz "CA")
Private Key / Public Key Verfahren	▪ Das Public Key Verfahren ist ein asymmetrisches, kryptographisches Verfahren, bei dem ein Schlüsselpaar zum Einsatz kommt. Dieses kryptografisches Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Daten die mit einem dieser Schlüssel verschlüsselt wurden, können nur mit dem anderen Schlüssel wieder entschlüsselt werden. ▪ Daten für den Empfänger werden mit dem öffentlichen Schlüssel (Public Key, Schlüssel im Zertifikat) verschlüsselt, und können nun nur noch durch den entsprechenden privaten Schlüssel entschlüsselt werden.
Public Key	▪ Der öffentliche Schlüssel/Public Key ist öffentlich über das Zertifikat zugänglich. Dieser Schlüssel wird zur Verschlüsselung von Daten oder zur Bestätigung der digitalen Signatur des Unterzeichners (Identifikation) verwendet. Mit dem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden.
Private Key	▪ Der private Schlüssel/Private Key ist nur dem Zertifikatsinhaber bekannt bzw. darf nur ihm zugänglich sein. Er wird für die Entschlüsselung von Daten und zur Erstellung einer digitalen Signatur verwendet.
Root Zertifikat	▪ Zertifikat einer übergeordneten Zertifizierungsstelle (Root-CA). Validiert die Gültigkeit aller untergeordneten Zertifikate.
Server Zertifikat	▪ Serverzertifikate gewährleisten die digitale Identifizierung eines Servers.
User Zertifikat	▪ Userzertifikate gewährleisten die digitale Identifizierung eines Users.
Self Signed Certificate	▪

Tabelle 1 Glossar / Definitionen, Akronym und Abkürzungen