ViMP 4.0

SSL Einrichtung in Apache 2.2

Verfasser:
ViMP GmbH

Inhaltsverzeichnis

Voraussetzungen

- Apache 2.x mit SSL (mod_ssl oder andere Implementierung)
- eine IP-Adresse, auf der noch keine HTTPS-Domain eingerichtet ist
- entsprechende Zertifikate des Servers und der CA

Eigene Zertifikate mit OpenSSL erstellen

Das Erstellen eines eigenen Server-Zertifikats sollte ausschließlich für Nicht-Produktiv-Systeme genutzt werden, da bei dieser Vorgehensweise Warnungen im Browser erscheinen. Für Produktiv-Systeme sollte das Server-Zertifikat bei einem renommierten Zertifikat-Anbieter erworben werden.

Selbst-signiertes Zertifikat erstellen

Als erstes erstellt man mit folgendem Kommando einen Schlüssel für den Server:

```
openssl genrsa -des3 -out server.key 4096
```

Dann muss die Signierungsanfrage des Zertifikats erstellt werden:

```
openssl req -new -key server.key -out server.csr
```

Das Kommando fragt eine Reihe von Einstellungen ab. Stellen Sie sicher, dass Sie unter `Common Name` den (registrierten) voll qualifizierten Domain Namen [Fully Qualified Domain Name http://de.wikipedia.org/wiki/FQDN] des Servers (oder die IP Adresse, falls kein FQDN vorhanden ist) angeben.

Die Vorgabewerte der Einstellungen sind in der `openssl.cnf` (z.B. zu finden unter `/etc/ssl/openssl.cnf`) gespeichert. Falls Sie eine Reihe an Zertifikaten erstellen wollen, können Sie die Werte dort entsprechend anpassen.

Nun signiert man die Signierungsanfrage (das folgende Beispiel stellt das Zertifikat für die nächsten 365 Tage aus):

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Als letztes erstellt man eine Kopie des Serverschlüssels ohne Passwort:

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

Die erstellten Dateien sind sehr sensibel und sollten vor fremden Zugriff geschützt werden

Zertifikat mit eigener Certificate Authority (CA) erstellen

Als erstes werden der Schlüssel und das Zertifikat der CA erstellt (das folgende Beispiel stellt das Zertifikat für die nächsten 365 Tage aus):

```
openssl genrsa -des3 -out ca.key 4096
openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

Der `Common Name` der CA und des Servers dürfen nicht übereinstimmen, ansonsten besteht ein Namenskonflikt, welcher zu Fehlern führen wird.

Als nächstes erstellt man einen Serverschlüssel und die Signierungsanfrage des Zertifikats:

```
openssl genrsa -des3 -out server.key 4096
openssl req -new -key server.key -out server.csr
```

Stellen Sie sicher, dass Sie unter `Common Name` den (registrierten) voll qualifizierten Domain Namen [Fully Qualified Domain Name http://de.wikipedia.org/wiki/FQDN] des Servers (oder die IP Adresse, falls kein FQDN vorhanden ist) angeben.

Nun signiert man die Signierungsanfrage (das folgende Beispiel stellt das Zertifikat für die nächsten 365 Tage aus):

```
openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out
server.crt
```

Beachten Sie, dass die Seriennummer des Zertifikats bei jedem Signierungsvorgang erhöht werden muss, ansonsten wird jeder Besucher Ihrer Seite mit einer zwischengespeicherten Version Ihres Zertifikats eine Warnung des Browsers erhalten.

Als letztes erstellt man eine Kopie des Serverschlüssels ohne Passwort:

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

Die erstellten Dateien sind sehr sensibel und sollten vor fremden Zugriff geschützt werden

Apache konfigurieren (mod_ssl)

Die folgenden Einstellungen gelten nur für mod_ssl [http://www.modssl.org] und können nicht oder nur bedingt auf andere SSL Implementierungen für Apache übertragen werden. Weiterführende Informationen zu den einzelnen Parametern finden Sie in der mod_ssl Referenz [http://www.modssl.org/docs/2.8/ssl_reference.html] bzw. der Apache Dokumentation [http://httpd.apache.org/docs/2.2/].

Mit der folgenden Zeile wird das Modul geladen:

```
LoadModule ssl_module              "modules/mod_ssl.so"
Grundlegende Beispiel-Konfiguration:
<IfModule ssl_module>
  SSLRandomSeed startup builtin
  SSLRandomSeed connect builtin

  Listen 443

  AddType application/x-x509-ca-cert .crt
  AddType application/x-pkcs7-crl    .crl

  SSLPassPhraseDialog  builtin

  SSLSessionCache           shmcb:/var/log/apache2/ssl.cache(512000)
  SSLSessionCacheTimeout    300

  SSLMutex default

  NameVirtualHost *:443
</IfModule>
```

Beispiel `VirtualHost`-Eintrag:

```
<IfModule ssl_module>
  <VirtualHost 127.0.0.1:443>
    ServerAdmin admin@example.org
    DocumentRoot "/var/www/framework/data/web"
    ServerName www.your-domain.org

    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile "/etc/apache2/ssl/server.crt"
    SSLCertificateKeyFile "/etc/apache2/ssl/server.key"

    <Directory "/var/www/framework/data/web">
      Options FollowSymLinks MultiViews
      AllowOverride All
      Order allow,deny
      Allow from All
    </Directory>
```

```
    ErrorLog /var/www/framework/logs/error.log
    CustomLog /var/www/framework/logs/access.log combined

  </VirtualHost>
</IfModule>
```

Für weitere Informationen zur SSL-Konfiguration des Apache ziehen Sie bitte die mod_ssl Dokumentation [http://www.modssl.org/docs/2.8/] bzw. die Apache Dokumentation [http://httpd.apache.org/docs/2.2/] zu Rate.

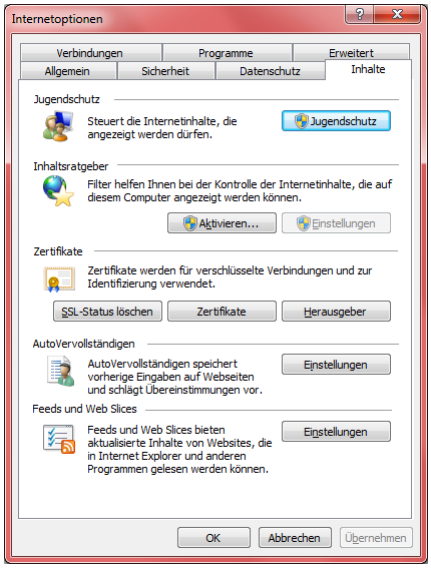
CA Zertifikat im Browser installieren

Damit die Warnung bezüglich der selbsterstellten Zertifikate der eigenen CA nicht mehr im Browser erscheint, muss das Zertifikat der CA im Browser installiert werden.

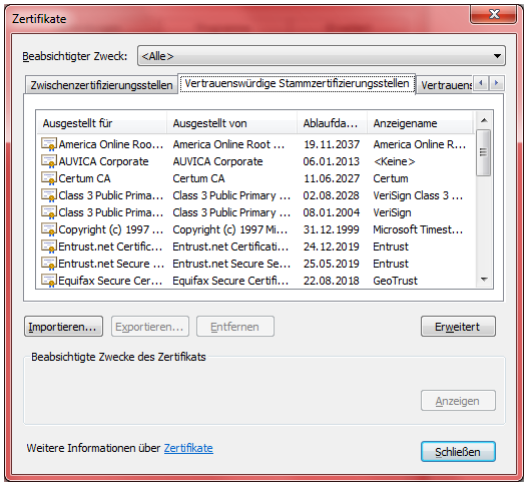
Internet Explorer

Je nach Version des Internet Explorers können die Dialoge leicht anders erscheinen. Der Anleitung liegt die derzeit aktuelle Version 8.0 zugrunde.

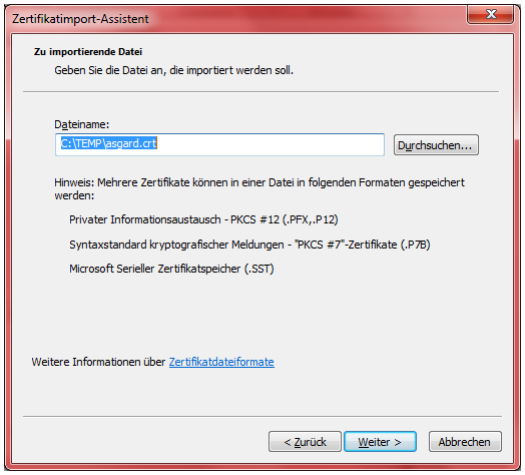
1. Öffnen Sie das Menü **Extras** und wählen den Punkt **Internetoptionen** aus.
2. Öffnen Sie den Karteireiter **Inhalte** und klicken Sie auf den Button **Zertifikate**.



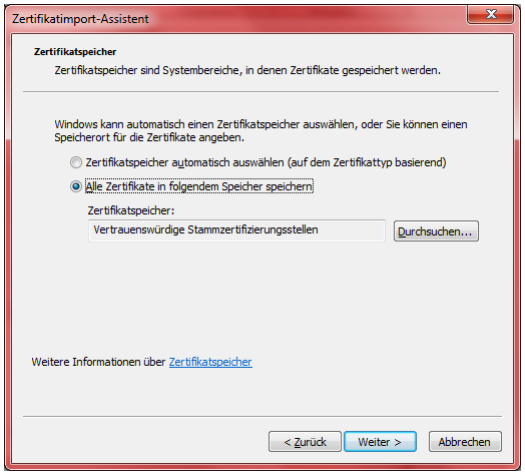
3. Öffnen Sie den Karteireiter **Vertrauenswürdige Stammzertifizierungsstellen** im Fenster Zertifikate und klicken Sie auf den Button **Importieren**.



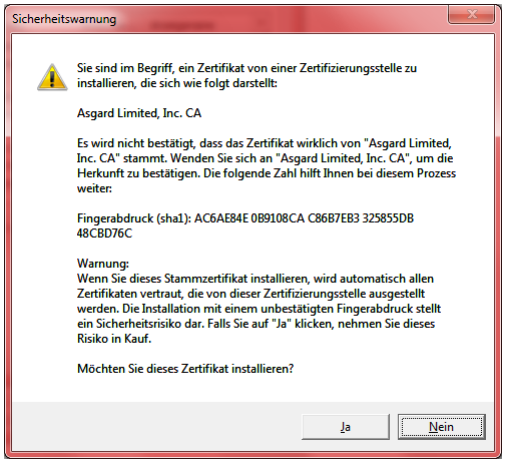
4. Wählen Sie auf Seite 2 des Zertifikatimport-Assistenten über den Button **Durchsuchen…** das Zertifikat der CA aus und klicken Sie dann auf den Button **Weiter**.



5. Auf der nächsten Seite des Zertifikatimport-Assistenten sollte der Punkt **Alle Zertifikate in den folgendem Speicher** speichern und der Zertifikatsspeicher **Vertrauenswürdige Stammzertifizierungsstellen** ausgewählt sein. Klicken Sie danach auf den Button **Weiter**.



6. Kontrollieren Sie auf der letzten Seite des Zertifikatimport-Assistenten Ihre Einstellungen und klicken Sie dann den Button **Fertig stellen**.
7. Bestätigen Sie die folgende Frage nach der Installation des Zertifikats der CA mit **Ja**.

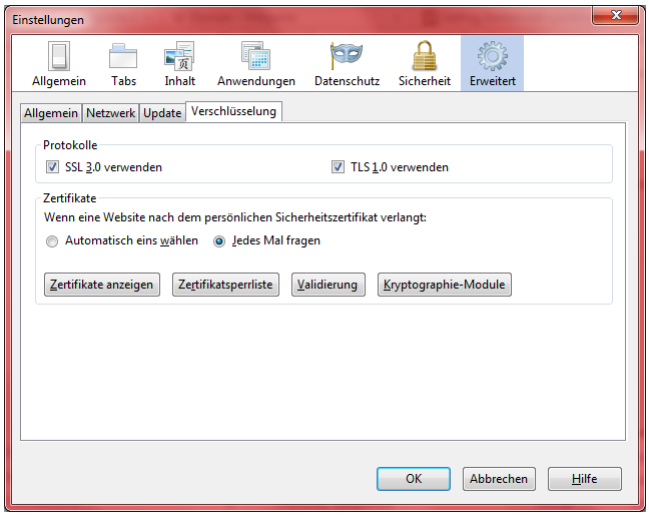


Damit ist das Zertifikat der CA im Internet Explorer installiert und es wird den mit der CA ausgestellten Zertifikaten vertraut.

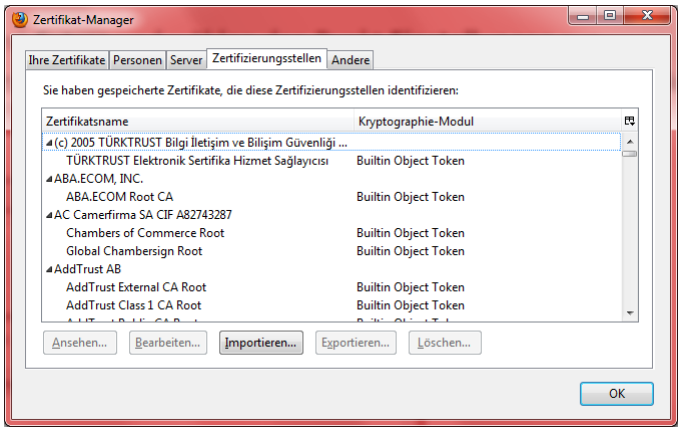
Firefox

Je nach Version des Firefox können die Dialoge leicht anders erscheinen. Der Anleitung liegt die derzeit aktuelle Version 3.5 zugrunde.

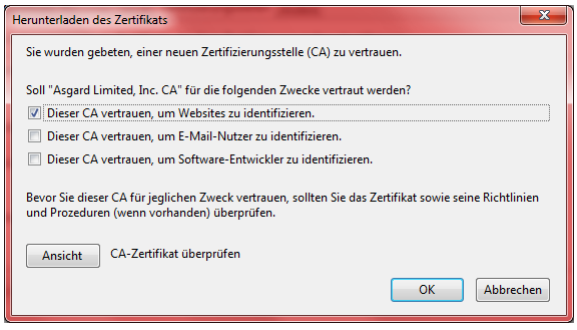
1. Öffnen Sie das Menü **Extras** und wählen Sie den Punkt **Einstellungen** aus.
2. Öffnen Sie den Karteireiter **Erweitert** und klicken Sie auf den Button **Zertifikate anzeigen**.



3. Öffnen Sie den Karteireiter **Zertifizierungsstellen** im Zertifikat-Manager und klicken Sie auf den Button **Importieren**.



4. Im sich öffnenden Datei-Auswahlfenster wählen Sie das Zertifikat der CA aus und klicken Sie auf den Button **Öffnen**.
5. Aktivieren Sie die Option **Dieser CA vertrauen, um Websites zu identifizieren**. Zusätzlich können Sie auch andere Optionen aktivieren. Klicken Sie bitte auf den Button **OK**.



Damit ist das Zertifikat der CA im Firefox installiert und es wird den mit der CA ausgestellten Zertifikaten vertraut.

Andere Browser

Wie Sie ein Zertifikat einer neuen Zertifizierungsstelle importieren, entnehmen Sie bitte der Dokumentation Ihres Browser.

Zertifikate und Flash-Plugin unter Windows

Leider existiert unter Windows im Flash-Plugin ein Fehler, so dass dieses in den Alternativ-Browsern Firefox, Chrome, Opera, etc. immer die Server-Zertifikate gegen die Zertifizierungsstellen des Internet Explorers prüft bzw. ob das Server-Zertifikat im Internet Explorer installiert ist.

Dadurch ist es **unumgänglich** alle selbst erstellen Zertifikate zusätzlich auch im Internet Explorer zu installieren. Bei Zertifikaten, die Sie bei einem renommierten Zertifikat-Anbieter erworben haben, ist dieser Schritt nicht nötig.