ViMP 3.5

SSL Configuration in Apache 2.2

Author:
ViMP GmbH

Table of Contents

Requirements

- Apache 2.x with SSL (mod_ssl or other implementation)
- IP address without existing HTTPS domain pointing to it
- Appropriate server and CA certificates

Create your own certificates with OpenSSL

The creation of your own server certificates should only be used for non-productive systems, as browser warnings will appear. For productive systems the server certificate should be purchased at qualified certificate providers.

Generate a self-signed certificate

First generate a server key with the following command:

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

Then create the signature inquiry of the certificate:

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

The command prompts a series of settings. Assure to enter the fully qualified domain name of the server at `Common Name` [Fully Qualified Domain Name http://en.wikipedia.org/wiki/FQDN] (or the IP address, if no FQDN exists).

The default values of the settings will be saved within the `openssl.cnf` file (e.g. to be found at `/etc/ssl/openssl.cnf`). If you want to create several certificates, you can adapt the values there.

Now sign the signature inquiry (the following example makes the certificate valid for 365 days):

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

At last make a copy of the server key without password:

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

The created files are very sensitive. Make sure to protect them from unauthorized access.

Generate a certificate with your own Certificate Authority (CA)

First create the key and the certificate of the CA (the following example makes the certificate valid for 365 days):

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

The `Common Name` of the CA and the server must not match, otherwise there will be a namespace conflict, causing errors.

Next, generate the server key and the signature inquiry of the certificate.

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

Assure to enter the fully qualified domain name of the server at `Common Name` [Fully Qualified Domain Name http://en.wikipedia.org/wiki/FQDN] (or the IP address, if no FQDN exists).

Now sign the signature inquiry (the following example makes the certificate valid for 365 days):

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

Note that the serial number of the certificate has to be increased at any signature procedure. Otherwise every visitor of your website with a cached version of your certificate will receive a warning.

At last make a copy of the server key without password:

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

The created files are very sensitive. Make sure to protect them from unauthorized access.

Apache configuration (mod_ssl)

The following settings are valid for mod_ssl [http://www.modssl.org] only and cannot or only partially be transferred to other Apache SSL implementations. Additional information about the individual parameters can be found in the mod_ssl reference [http://www.modssl.org/docs/2.8/ssl_reference.html] or the Apache documentation [http://httpd.apache.org/docs/2.2/].

The following command loads the module:

```
LoadModule ssl_module              "modules/mod_ssl.so"

A basic configuration sample:
<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>
```

`VirtualHost` entry sample:

```
<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>
```

For further information about the Apache SSL configuration please consult the mod_ssl documentation [http://www.modssl.org/docs/2.8/] or the Apache documentation [http://httpd.apache.org/docs/2.2/].

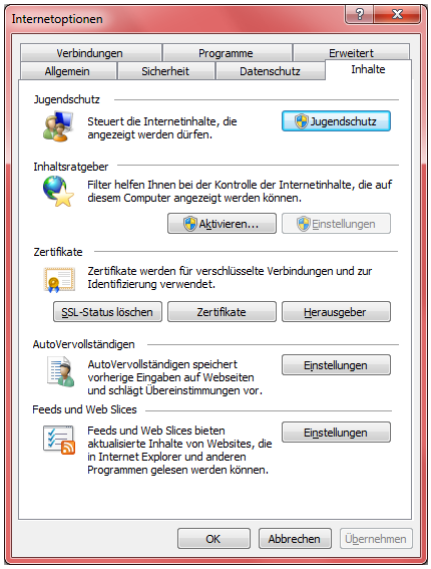
Browser installation of the CA certificate

To disable the warnings produced by the self-generated certificate of your own CA, the certificate of the CA must be installed in the browser.

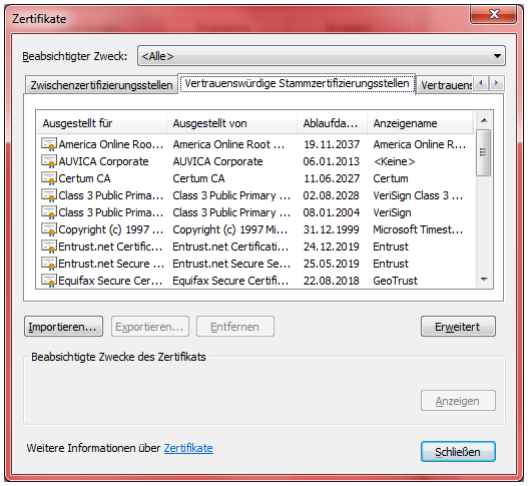
Internet Explorer

According to the version of Internet Explorer the dialogs might appear slightly different. The tutorial is based on version 8.0.

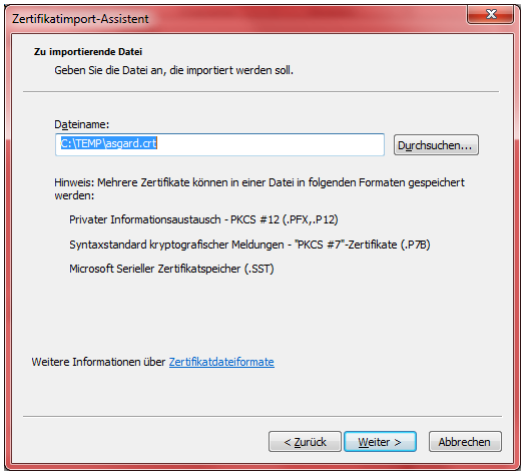
1. Open the **Extras** menu and click **Internet options**.
2. Open the **Contents** tab and click the button **Certificates**.



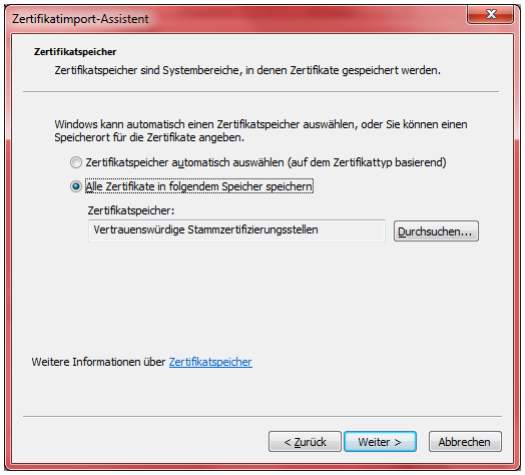
3. Open the **Trusted Root Certification Authorities** tab within the certificates window and click the **Import** button.



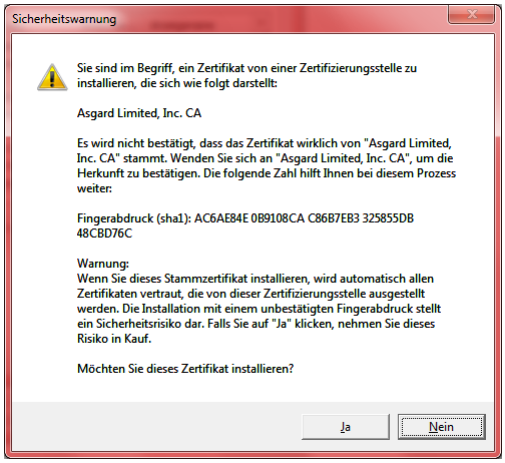
4. Select the certificate of the CA on page 2 of the certificate import assistant via the **Browse…** button, then click **Next**.



5. On the next page of the certificate import assistant **Save all certificates in the following storage** and the certificate storage **Trusted Root Certification Authorities** should be selected. Click the **Next** button.



6. Check your settings on the last page of the certificate import assistant, then click the **Finish** button.
7. Confirm the following question after the installation of your certificate of the CA with **Yes**.

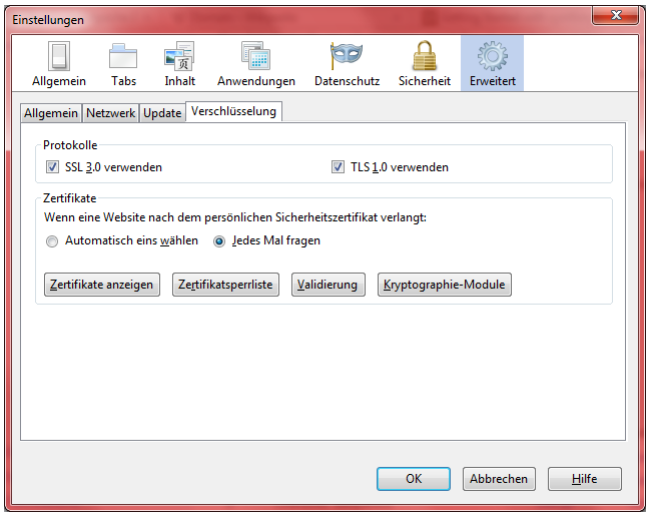


Now the certificate of the CA is installed in Internet Explorer and certificates of the CA will be handled as trusted certificates.

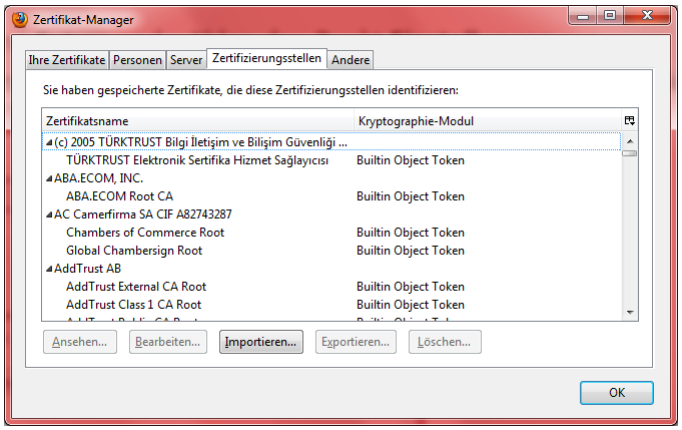
Firefox

According to the version of Firefox the dialogs might appear slightly different. The tutorial is based on version 3.5.

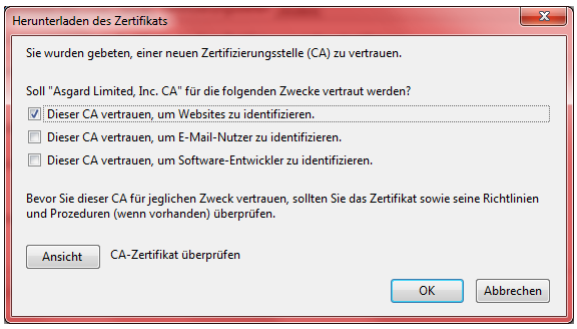
1. Open the **Extras** menu and click **Settings**.
2. Open the **Advanced** tab and click the button **Display certificates**.



3. Open the **Certification authorities** tab within the certificate manager and click **Import**.



4. Select the certificate of the CA within the file manager window and click the **Open** button.
5. Activate the option **Trust this CA to identify web sites**. You can also activate additional options, if necessary. Then click **OK**.



Now the certificate of the CA is installed in Firefox and certificates of the CA will be handled as trusted certificates.

Other Browsers

Please consult the documentation of the other browser to install certificates of a new CA.

Certificates and Flash plugin on Windows

Unfortunately there is a bug within the Flash plugin on Windows. On Windows Flash always checks the server certificates against the certification authorities of the Internet Explorer and not against the certification authorities of the other currently used browsers like Firefox, Chrome, Opera, etc.

This makes it **essential** to install the self-generated certificates always in Internet Explorer as well, even if you don't use that browser. With certificates of trusted certificate providers this additional step is not necessary.