

ViMP 4.0

SSL Configuration in Apache 2.2

Author: ViMP GmbH



Table of Contents

Requirements
Create your own certificates with OpenSSL 4
Generate a self-signed certificate 4
Generate a certificate with your own Certificate Authority (CA) 4
Apache configuration (mod_ssl)
Browser installation of the CA certificate
Internet Explorer
Firefox
Other Browsers
Certificates and Flash plugin on Windows



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 sampl <ifmodule ssl_module=""> SSLRandomSeed startup bui SSLRandomSeed connect bui</ifmodule>	e: ltin ltin
Listen 443	
AddType application/x-x50 AddType application/x-pkc	9-ca-cert .crt s7-crl .crl
SSLPassPhraseDialog buil	tin
SSLSessionCache SSLSessionCacheTimeout	shmcb:/var/log/apache2/ssl.cache(512000) 300
SSLMutex default	
NameVirtualHost *:443 	

VirtualHost entry sample:

```
</li
```



ErrorLog /	/var/www/framework/logs/error.log	
CustomLog	<pre>/var/www/framework/logs/access.log</pre>	combine

</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.

Zertifikate	-			×
Beabsichtigter Zweck: <alle:< td=""><td>></td><td>mmzertifizierur</td><td>igsstellen Vertrauen</td><td>•</td></alle:<>	>	mmzertifizierur	igsstellen Vertrauen	•
Ausgestellt für	Ausgestellt von	Ablaufda	Anzeigename	^
America Online Roo	America Online Root AUVICA Corporate Certum CA Cass 3 Public Primary Class 3 Public Primary Copyright (c) 1997 M Entrust.net Certificat Entrust.net Secure Se Equifax Secure Certifi	19.11.2037 06.01.2013 11.06.2027 02.08.2028 08.01.2004 31.12.1999 24.12.2019 25.05.2019 22.08.2018	America Online R <keine> Certum VeriSign Class 3 VeriSign Microsoft Timest Entrust Entrust GeoTrust</keine>	E
Importeren Entfernen Erweitert Beabsichtigte Zwecke des Zertifikats Anzeigen				
Weitere Informationen über 2	<u>'ertifikate</u>		Schließ	en



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

Zertifikatimport-Assistent
Zu importierende Datei
Geben Sie die Datei an, die importiert werden soll.
Dateiname:
C:\TEMP\asgard.crt Durchsuchen
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Microsoft Serieller Zertifikatspeicher (.SST)
Weitere Informationen über Zertifikatdateiformate
< <u>Z</u> urüdk <u>Weiter</u> Abbrechen

 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**.

Sicherheits	warnung
	Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt: Asgard Limited, Inc. CA Es wird nicht bestätigt, dass das Zertifikat wirklich von "Asgard Limited, Inc. CA" stammt. Wenden Sie sich an "Asgard Limited, Inc. CA", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter: Fingerabdruck (sha1): AC6AE84E 089108CA C8687EB3 325855D8 48CB076C Warnung: Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einen unbestätigten Fingerabdruck stellt ein Sicherheitsrisko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.
	Ja Ja

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**.

e Zertifikate Personen Server Zertifizierungsstellen Ar	ndere	
Sie haben gespeicherte Zertifikate, die diese Zertifizierung	sstellen identifizieren:	
Zertifikatsname	Kryptographie-Modul	E.
4 (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği		*
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token	
▲ABA.ECOM, INC.		
ABA.ECOM Root CA	Builtin Object Token	
AC Camerfirma SA CIF A82743287		
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	
▲AddTrust AB		
AddTrust External CA Root	Builtin Object Token	
AddTrust Class 1 CA Root	Builtin Object Token	-
<u>Ansehen</u> <u>B</u> earbeiten <u>Importieren</u> Expo	ortieren Löschen	
Ansenen Dearbeiten Importieren Expo	Loschen	

- 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.

Herunterladen des Zertifikats	x
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.	
Soll "Asgard Limited, Inc. CA" für die folgenden Zwecke vertraut werden?	
Dieser CA vertrauen, um Websites zu identifizieren.)
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.	
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.	
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlin und Prozeduren (wenn vorhanden) überprüfen.	ien
Ansicht CA-Zertifikat überprüfen	
OK Abbrec	hen

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.