



## Konfiguration Apache Webserver für SSL

Voraussetzung für dieses Tutorial ist ein installierter Apache HTTPD Webserver, wir verwenden die zurzeit aktuelle Version 2.4.16. Dieser beinhaltet OpenSSL in der Version 1.0.2d.

Hinweise:

1. Wir setzen einen anhand der Anleitung „Installation & Konfiguration Apache Webserver + PHP“ voraus – das gilt insbesondere für die Verzeichnisstruktur. Sie können diese selbstverständlich an Ihre Gegebenheiten anpassen.
2. Wir schreiben unsere Tutorials immer im LIVE-Betrieb, d.h. wir schreiben nie blind ohne Ausprobieren eine Anleitung. Hier beim Erzeugen eines Zertifikats ist das natürlich schwierig – wir können nicht willkürlich eins für „meineschule.at“ erzeugen lassen, da wir diese Domäne nicht besitzen. Das Zertifikat wird daher auf „skrejci.com“ ausgestellt. Passen Sie auch hier den Domänennamen jeweils dem Ihrigen an!

Wir bei schultermine.com verwenden, wie viele andere Webseiten auch, Zertifikate von StartCom. Zurzeit sind wir Class 2 zertifiziert.

Wird ein Zertifikat für nur eine Domäne benötigt, reicht eine Class 1 Zertifizierung. Diese ist kostenlos, es genügt eine einfache Registrierung – und daher sehr praktisch für ebendiese Zwecke!

Dieses Tutorial führt Sie nun in **fünf Schritten** zu einem Webserver, der Webseiten an SSL-Verbindungen bereitstellt:

1. StartCom: Email-Adresse validieren
2. StartCom: Domäne validieren
3. StartCom: Private Key generieren und Zertifikat erstellen
4. Apache für SSL konfigurieren
5. Firewall für eingehende SSL-Verbindungen konfigurieren

Um eine SSL-Verbindung auf Ihrem Webserver bereitstellen zu können, benötigen Sie...

- ein Zertifikat (ssl.crt),
- einen zugehörigen privaten Schlüssel (ssl.key),
- ein Serverzertifikat (Zertifikatskette) sowie
- ein Stammzertifikat (Certificate Authority, CA).



(Die Dateinamen in Klammern sind selbstverständlich beliebig – wir verwenden, wie im Folgenden von StartCom vorgeschlagen, eben diese angegebenen.)

Navigieren Sie zur Seite [startssl.com](http://startssl.com).

**StartSSL™ - The Swiss Officer's Knife of Digital Certificates & PKI**

Welcome to StartSSL™ PKI

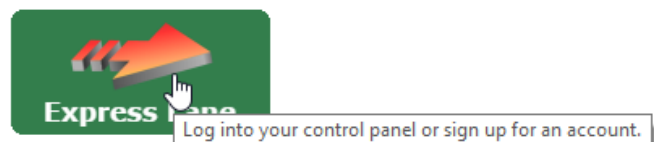
StartSSL™ is the trade mark of the StartCom® Certification Authority - a leader of the digital certification industry. We provide you with everything from free low-assurance SSL certificates up to the most advanced PKI and security solutions for your business and personal use.

- StartSSL™ Free (Class 1)**  
128/256-bit Encryption, 1 Year Validity  
Highest Level Third Party Assurance  
No Charge, Unlimited + 100% Free
- StartSSL™ EV**  
High Level Trust Indicator  
Time Limited Offer  
Only **us\$199,90**
- StartSSL™ Extended Validation**  
128/256-bit Encryption, 2 Years Validity  
Highest Level Third Party Assurance  
Green Extended Trust Indicator  
Multiple Domain Names (UCC)  
Special Offer - **US\$ 199,90**
- StartSSL™ Verified (Class 2)**  
128/256-bit Encryption, 2 Years Validity  
Legitimate SSL/TLS + S/MIME + Object Code  
Wild Cards, Multiple Domain Names (UCC)  
Unlimited Certificates - **US\$ 59,90**
- Hardware**  
Aladdin® USB eToken Pro  
Aladdin® Smart Cards + Reader  
Original Driver Software + PKI Client  
Enterprise PKI Customized Solutions
- High Protection**  
StartSSL™ High Level Protection  
No MD5 Hashes, Weak Key Scans  
Minimum 2048-bit Strong RSA Keys
- Authentication**  
StartSSL™ Authentication SSL Protected  
Open Identity Authentication Provider  
Click here to log into your StartSSL™ Account
- Easy Enrollment**  
Sign-up and you will receive right away an S/MIME client-certificate and a digital StartSSL™ Open Identity without charge during the easy three-step enrollment!
- Internationally Recognized**  
WebTrust for CAs + WebTrust EV Certified  
Recognized by major browsers + software vendors

© Copyright (c) 2004 - 2013 by StartCom Ltd. (Start Commercial Limited) All rights reserved. BetterTrust™, StartCom® and StartSSL® are trademarks of StartCom Ltd.  
WebTrust is a trademark of the Canadian Institute of Chartered Accountants (CICA). All other product names mentioned herein and throughout the entire site are trademarks of their respective owners.

Klicken Sie rechts oben auf das Tür-Schlüsselsymbol. Klicken Sie anschließend auf „Express Lane“.

**...or get a StartSSL™ Free server certificate real quick!**  
Follow the Express Lane which will guide you through all the necessary steps. Choose this option only if this is your first time here, otherwise log into your account above.



### Schritt 1: EMail-Adresse validieren

Nach der Registrierung müssen Sie über den „Validations Wizard“ Ihre Email-Adresse verifizieren. Klicken Sie dazu auf „Validations Wizard“ und wählen unter „Type“ die „Email Address Validation“ aus.



Tool Box

Certificates  
Wizard

Validations  
Wizard

- Select the type and attribute of validation
- Please note that you might need to have

Type:


Continue >>>

Geben Sie Ihre Email-Adresse ein und klicken Sie auf Continue.  
Bitte bedenken Sie, dass diese Email-Adresse später im Zertifikat für Ihren Webserver aufscheinen wird – verwenden Sie besser eine offizielle (Schul-)Email-Adresse als eine private.

Email:

Continue >>>

Sie bekommen im Anschluss ein Email mit einem Verification Code zugeschickt.

 **StartCom CertMaster**  
Your Authentication Code, 18 Aug 2015 12:14

**Your Authentication Code, 18 Aug 2015 12:14**

StartCom CertMaster <certmaster@startcom.org>

Die unnötigen Zeilenumbrüche des Nachrichtentextes wurden automatisch entfernt.

Gesendet: Di 18.08.2015 11:15

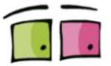
An: office@skrejci.com

This mail is intended for the person who requested verification of email ownership at StartSSL™ (<http://www.startssl.com>).

Your verification code is PRI44tOj1DGFvTUo Copy and paste this code now into the form at your open browser window.

Thank you!

StartCom Ltd.  
StartSSL™ Certification Authority



Kopieren Sie den Code und fügen Sie ihn im entsprechenden Feld

### Complete Validation

- A verification code has been sent to "office@skrejci.com".
- Please check your email account now and enter the code into the

Verification Code:

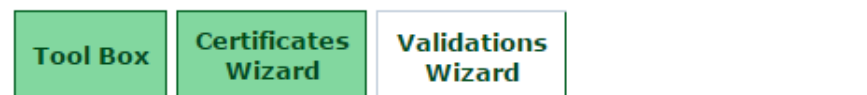
PRI44tOj1DGFvTUo

Continue >>>

Klicken Sie auf Continue und anschließend auf Finish.

### Schritt 2: Domäne validieren

Für die Validierung Ihrer Domäne gehen Sie analog wie bei der Validierung für die Email-Adresse vor. Wählen Sie im „Validations Wizard“ nun „Domain Name Validation“ aus.



### Select Validation

- Select the type and attribute of validation you'd like to perform
- Please note that you might need to have instant access to your in image format ready.

Type:

- Domain Name Validation
- Email Address Validation
- Domain Name Validation
- Personal Identity Validation
- Organization Validation (Requires Personal Identity)
- Extended Validation (Requires Personal Identity)

This wizard will guide you through the process of validating...

Geben Sie nun Ihre Domäne ein und klicken Sie auf Continue.

http://  .

Continue >>>

Sie erhalten eine Liste aller beim Registrar eingetragenen Email-Kontaktadressen. Wählen Sie diejenige aus, auf die Sie Zugriff haben und klicken Sie auf „Continue“.



### Select Verification Email

- Select the email address for verification of domain ownership from below.

- Verification Email:**
- postmaster@skrejci.com
  - hostmaster@skrejci.com
  - webmaster@skrejci.com
  - support@domainbox.com
  - office@skrejci.com
  - support@hosteurope.de

**Continue >>>**

Sie erhalten wiederum ein Email mit einem Verification Code.  
Kopieren Sie diesen Code in die Zwischenablage und fügen Sie ihn auf der Homepage ein.

### Complete Validation

- A verification code has been sent to "office@skrejci.com".
- Please check your email account now and enter the code into the text field below.

**Verification Code:**

8DsQpXqtE3c1fPzz

**Continue >>>**

Diese Domänen-Validierung ist nun 30 Tage lang gültig. In diesem Zeitraum müssen Sie das Zertifikat ausstellen, ansonsten müssen Sie die Domäne erneut validieren.

### Validation Success

- You have successfully authenticated domain "skrejci.com".
- You will be able to use this verification for the next 30 days, after which it expires and must be renewed.

**Finish >>>**

## Schritt 3: Zertifikat anfordern

Um ein Zertifikat für Ihre Domäne zu erstellen, klicken Sie nun auf „Certificates Wizard“ und wählen aus der Liste „Web Server SSL/TLS Certificate“ aus.



**Tool Box**   **Certificates Wizard**   **Validations Wizard**

### Select Certificate Purpose

- Make sure you have already validated a domain name or email address: Select the "**Validations Wizard**" for this task.
- Depending on your preferences and type of software, you need to have request (CSR) ready for submission.

**Certificate Target:**

- S/MIME and Authentication Certificate
- Web Server SSL/TLS Certificate**
- XMPP (Jabber) SSL/TLS Certificate
- Object Code Signing Certificate

Im nächsten Schritt wird Ihr privater Schlüssel erzeugt. Sie benötigen ein Passwort (Länge zwischen 10 und 32 alphanumerische Zeichen). Notieren Sie sich dieses Passwort gut! Belassen Sie aus Sicherheitsgründen die Keysize unbedingt bei 4096 Byte und den Hash-Algorithmus bei sha2!

**Key Password:**

**Confirm Password:**

**Keysize:**

**Secure Hash Algorithm:**

**Skip >>>**   **Continue >>>**

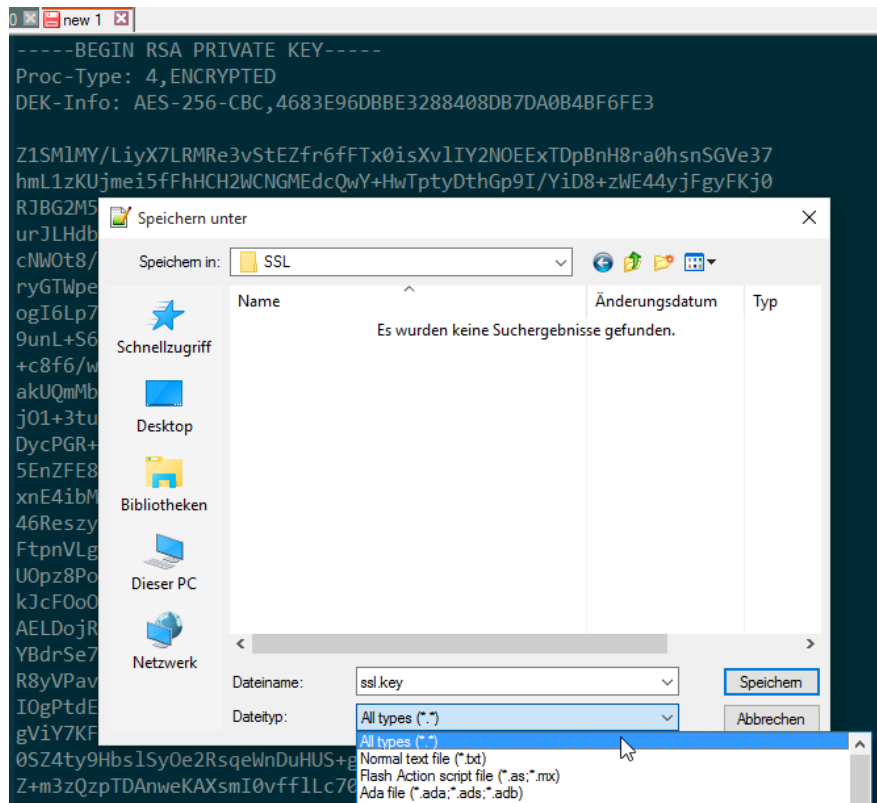
Der private Key wird nun generiert und in einer Textarea dargestellt. Kopieren Sie den gesamten Inhalt in einen Texteditor Ihrer Wahl und speichern Sie die Datei unter dem Namen ssl.key ab!

### Save Private Key

- Copy and paste the content from the textbox below into a file and save it as **ssl.key**
- Make sure, that you do not alter the content and you did not add any spaces! Save format (plain text).
- Allowed are only letters and numbers, without spaces!
- Decrypt the private key with the OpenSSL utility: **openssl rsa -in ssl.key -out s** the utility from the Tool Box.

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-256-CBC,4683E96DBBE3288408DB7DA0B4BF6FE3  
  
Z1SMIMY/LiyX7LRMRe3vStEZfr6fFTx0isXvIIY2NOEExTDpBnH8ra0hsnSGVe37  
hmL1zKUjmei5fFhHCH2WCNGMEdcQwY+HwTptyDthGp9I/YiD8+zWE44yJFgyFKj0  
RJBG2M5cR27xuP6UL5bygiPt5EV6j/aEOfxdqUfiKeMjKameBePkCd7W6iaQFTG6
```

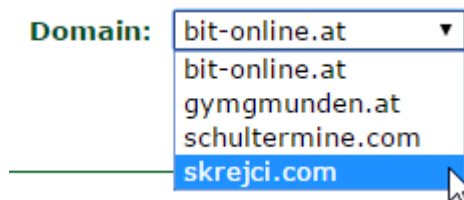
**Continue >>>**



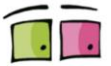
Je nach verwendetem Editor müssen Sie den Dateityp auf „All types (\*.\*)“ umstellen, damit die Datei nicht fälschlicherweise den Dateinamen „ssl.key.txt“ erhält.

Klicken Sie nun auf „Continue“.

Nach der Erstellung des Private Keys wird jetzt das Zertifikat für Ihre Domäne beantragt. Wählen Sie aus der Drop Down Liste Ihre zuvor validierte Domäne aus.



Das nächste Dialogfeld sieht je nach bei StartSSL gewähltem Paket bzw. je nach Anzahl der verfügbaren Domänen verschieden aus. Je nachdem wie Ihre Domäne lautet, müssen Sie hier die Subdomain eintragen – im Allgemeinen ist dies „www“. Damit wird das Zertifikat automatisch auf „skrejci.com“ und „www.skrejci.com“ ausgestellt.



### Add Domains

- You may add additional domains and sub domain which have been v
- Note: The additional entries will appear as DNS Alternative Names i

Domain:

https://  .

[Continue >>>](#)

Sind Sie berechtigt, ein Wildcard-Zertifikat auszustellen (ein Zertifikat, dass für alle Subdomains Ihrer Domäne gilt), so tragen Sie statt www ein Sternchen \* ein.

### Add Domains

- You may add additional domains and sub domain which have been v
- Note: The additional entries will appear as DNS Alternative Names

Domain:

https://  .

[Continue >>>](#)

Klicken Sie anschließend auf „Continue“. Es wird eine Zusammenfassung angezeigt.

### Ready Processing Certificate

- We have gathered enough information in order to sign your certificate.
- The common name of this certificate will be set to **\*.skrejci.com**.
- The certificate will have the following host names supported:
  1. **skrejci.com**
  2. **\*.skrejci.com**
- Please click on *Continue* in order to process the certificate.

[Continue >>>](#)

Mit einem weiteren Klick auf „Continue“ wird das Zertifikat erzeugt.





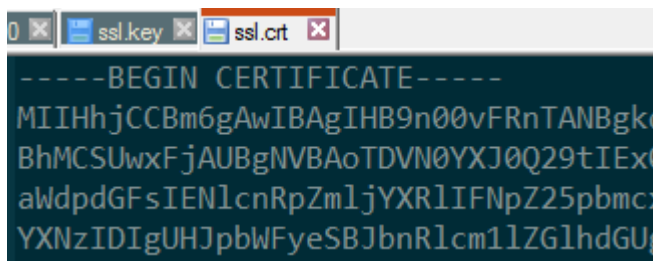
## Retrieve Certificate

- You must have the corresponding private key or request pending in order to retrieve the certificate.
- Make sure to backup the certificate including the private key to some safe location.


### Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIHhjCCBm6gAwIBAgIHB9n00vFRnTANBgkqhkiG9w0BAQsFADCBjDELM  
AkGA1UE  
BhMCSUwxFjAUBgNVBAoTDVN0YXJ0Q29tIEx0ZC4xKzApBgNVBAstiINlY3  
VyZSBE  
aWdpdGFsIENlcnRpZmljYXRlIFNpZ25pbmcxODQ2BgNVBAMTL1N0YXJ0Q  
29tIENS
```

Speichern Sie das Zertifikat wie vorher in einer Textdatei, diesmal unter dem Namen „ssl.crt“.



Nun benötigen Sie noch die Root-Zertifikate. Wählen Sie unter „Toolbox“ den Menüeintrag „StartCom CA Certificates“ aus.

**Tool Box** Certificates Wizard Validations Wizard 

**The Toolbox**

**StartCom CA Certificates**

- If you want to import one or more CA certificates into your browser click on the link of the certificate in question. Make sure to edit the trust settings of each imported certificate.
- In order to save the certificates for your server, select the link by right clicking on it and selecting "Save Link As..." from the menu.
- **StartCom Root CA** (PEM encoded)
- **StartCom Root CA** (DER encoded)
- **Server Certificate Bundle with CRLs** (PEM encoded)
- **Class 1 Intermediate Server CA**
- **Class 2 Intermediate Server CA**
- **Class 3 Intermediate Server CA**
- **Extended Validation Server CA**
- **Class 1 Intermediate Client CA**
- **Class 2 Intermediate Client CA**
- **Class 3 Intermediate Client CA**
- **Class 2 Code Signing CA**
- **Class 3 Code Signing CA**

Laden Sie als erstes das „StartCom Root CA (PEM encoded)“ herunter. Dieses erhält den Namen „ca.pem“.



- **StartCom Root CA (PEM encoded)**
  - **StartCom Root CA**
  - **Server Certificate**
  - **Class 1 Intermediate**
  - **Class 2 Intermediate**
  - **Class 3 Intermediate**
- Link in neuem Tab öffnen  
Link in neuem Fenster öffnen  
Link in Inkognito-Fenster öffnen  
Link speichern unter...

Anschließend wählen Sie das Server Zertifikat der entsprechenden Klasse aus. Diese finden Sie rechts unter „Validations“ je nach Anzahl der grünen Häkchen.

Validations			
<b>Class 1:</b>	✓	<b>Class 2:</b>	✓
<b>Class 3:</b>	✗	<b>EV:</b>	✗

In diesem Fall (grünes Häkchen bei Class 1 und Class 2) wird das Serverzertifikat „Class 2 Intermediate Server CA“ benötigt.

- **Class 1 Intermediate Server CA**
  - **Class 2 Intermediate Server CA**
  - **Class 3 Intermediate Server CA**
  - **Extended Validation Server CA**
  - **Class 1 Intermediate Client CA**
  - **Class 2 Intermediate Client CA**
  - **Class 3 Intermediate Client CA**
- Link in neuem Tab öffnen  
Link in neuem Fenster öffnen  
Link in neuem privaten Fenster öffnen  
Lesezeichen für diesen Link hinzufügen  
Ziel speichern unter...

Sind Sie „nur“ Class 1 validiert, wählen Sie bitte das „Class 1 Intermediate Server CA“. Speichern Sie dieses Zertifikat unter dem vorgeschlagenen Dateinamen, z.B. „sub.class2.server.ca.pem“).

Sie haben nun insgesamt vier Dateien erzeugt bzw. heruntergeladen.

ca.pem	18.08.2015 11:40	PEM-Datei	3 KB
ssl	18.08.2015 11:40	Sicherheitszertifikat	3 KB
ssl.key	18.08.2015 11:23	KEY-Datei	4 KB
sub.class2.server.ca.pem	18.08.2015 11:43	PEM-Datei	3 KB

#### Schritt 4: Installation SSL am Webserver

Diese vier Dateien kopieren Sie nun auf Ihren Webserver in das Verzeichnis „c:\Webserver\Configuration“.

Erstellen Sie nun in diesem Verzeichnis eine Datei namens „ssl\_passphrase.bat“ als Textdatei und öffnen Sie diese zur Bearbeitung. Schreiben Sie in diese Datei folgende Zeile:



@echo XXXX

Ersetzen Sie das XXXX dabei durch das Passwort des privaten Schlüssels! Bei Aufruf dieser Batch-Datei wird mittels dem echo-Befehl das Passwort auf der Kommandozeile ausgegeben, so bekommt der Webserver Zugriff auf den privaten Schlüssel. Speichern Sie die Datei und schließen Sie sie!

```
ssl_passphrase.bat x  ssl.key x  ssl.crt  
1 @echo 39c0e5cbe94e6d3d
```

Öffnen Sie nun am Webserver die Apache-Konfigurationsdatei „httpd.conf“ im Verzeichnis „c:\Webserver\Apache24\conf“.

Navigieren Sie zu der Stelle in der Datei, an der die zusätzlichen Module geladen werden. Binden Sie die beiden Module „mod\_ssl“ und „mod\_socache\_shmcb“ ein.

```
165 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so  
166 LoadModule ssl_module modules/mod_ssl.so
```

Navigieren Sie nun nach(fast ganz) unten zur Zeile „Include conf/extra/httpd-ssl.conf“. Entfernen Sie das Raute-Symbol davor, sodass die Zeile interpretiert und die httpd-ssl.conf – Datei mit in die Konfiguration aufgenommen wird.

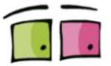
```
Include conf/extra/httpd-ssl.conf
```

Stellen Sie auch sicher, dass die folgenden Zeilen etwas unterhalb nicht auskommentiert sind.

```
<IfModule ssl_module>  
  SSLRandomSeed startup builtin  
  SSLRandomSeed connect builtin  
</IfModule>
```

Speichern und schließen Sie diese Datei, öffnen Sie statt dessen die Datei „httpd-ssl.conf“ im Verzeichnis „c:\Webserver\Apache24\conf\extra“.

In dieser Datei werden – ähnlich wie in der httpd-vhosts.conf – Datei – die Virtual Hosts für die SSL-Verbindungen angeben. Zuerst folgt ein Block mit den allgemeinen SSL-Einstellungen, hier im folgenden wieder eine Beispielformatierung ohne Gewähr:



```
Listen *:443
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-
AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-
RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-
AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-
AES256-SHA:AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128:AES256:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!3DES:!MD5:!PSK:!ECDHE-RSA-RC4-
SHA:!ECDHE-ECDSA-RC4-SHA:!RC4-SHA
SSLHonorCipherOrder on
SSLProtocol all -SSLv3
SSLProxyProtocol all -SSLv3
SSLPassPhraseDialog "exec:C:/WebServer/Configuration/ssl_passphrase.bat"
SSLSessionCache "shmcb:c:/WebServer/Logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300
```

Hier kommt die zuvor erstellte „ssl\_passphrase.bat“ zum Einsatz.

Anschließend an diese allgemeinen Konfigurationen folgt die Definition der einzelnen Hosts. Auch hier geben wir Ihnen wieder eine mögliche Beispielkonfiguration zur Vorlage wieder:

```
<VirtualHost *:443>
  DocumentRoot "c:/WebServer/wwwRoot/www.skrejci.com.ssl"
  ServerName www.skrejci.com:443
  ServerAdmin postmaster@skrejci.com
  ErrorLog "c:/WebServer/Logs/www.skrejci.com.ssl.error.log"
  TransferLog "c:/WebServer/Logs/www.skrejci.com.ssl.access.log"
  SSLEngine on
  SSLCertificateFile "c:/WebServer/Configuration/ssl.crt"
  SSLCertificateKeyFile "c:/WebServer/Configuration/ssl.key"
  SSLCertificateChainFile "c:/WebServer/Configuration/sub.class2.server.ca.pem"
  SSLCACertificateFile "c:/WebServer/Configuration/ca.pem"
  <Directory "c:/WebServer/wwwRoot/www.skrejci.com.ssl">
    Options None
    AllowOverride All
    Require all granted
    DirectoryIndex index.php index.html
  </Directory>
  <FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
  </FilesMatch>
  <Directory "c:/WebServer/Apache24/cgi-bin">
    SSLOptions +StdEnvVars
  </Directory>
  BrowserMatch "MSIE [2-5]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
  CustomLog "c:/WebServer/Logs/www.skrejci.com.ssl_request.log" \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

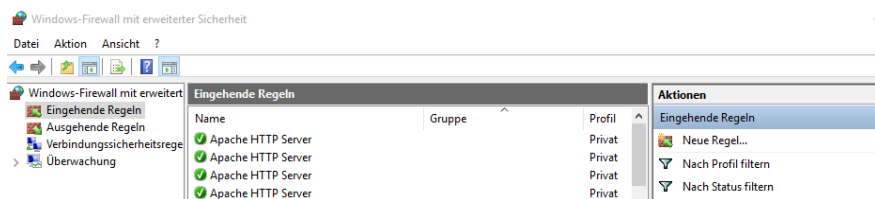


Wie bei den „normalen“ Virtual Hosts werden die SSL-Pendants über die Direktive „ServerName“ identifiziert. Die Zertifikate bzw. der private Key werden über die entsprechenden SSLCertificate- bzw. SSLCertificate-Direktiven eingebunden. Anschließend werden die Optionen für den DocumentRoot genauso wie in der httpd-vhosts.conf festgelegt.

### Schritt 5: Firewall für SSL einrichten

Damit eingehende SSL-Anforderungen nicht geblockt werden, muss standardmäßig Port 443 auf der lokalen Firewall (und selbstverständlich auch auf allfälligen vorgeschalteten Firewalls durchgeroutet und) freigeschaltet werden.

Öffnen Sie dazu die „Windows-Firewall mit erweiterter Sicherheit“ auf dem Server. Navigieren Sie zu „eingehende Regeln“ und klicken Sie rechts auf „Neue Regel...“.

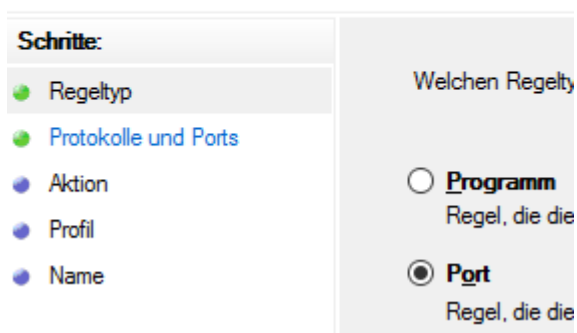


Aktivieren Sie im ersten Schritt „Port“,



#### Regeltyp

Wählen Sie den Typ der zu erstellenden Firewallregel aus.



im nächsten Dialogfenster geben Sie bei „bestimmte lokale Ports“ die Zahl 443 an.



Betrifft diese Regel TCP oder UDP?

**TCP**

**UDP**

Gilt diese Regel für alle lokalen Ports oder für bestimmte lokale Ports?

**Alle lokalen Ports**

**Bestimmte lokale Ports:**

Beispiel: 80, 443, 5000-5010

Im nächsten Dialogfeld belassen Sie „Verbindung zulassen“, im wiederum nächsten Dialogfeld belassen Sie alle drei Profiltypen „Domäne“, „Privat“ und „Öffentlich“ aktiviert. Im letzten Schritt vergeben Sie eine eindeutige Bezeichnung, und klicken Sie auf Fertig stellen.

Name:

Ab sofort lässt Ihr Server Anfragen auf dem Standard-SSL Port 443 zu.

### Fertig!

Testen Sie den Zugriff nun, indem Sie Ihren Server mit vorangestelltem „https“ aufrufen!

**Wichtiger Hinweis:** In näherer Vergangenheit sind immer wieder teil gravierende Sicherheitsprobleme im Umgang mit SSL aufgetreten. Prüfen Sie daher in halbwegs regelmäßigen Abständen Ihren SSL-Server auf Sicherheit! Navigieren Sie z.B. zur Seite [www.ssllabs.com/ssltest](http://www.ssllabs.com/ssltest). Geben Sie hier Ihren Domännennamen an und klicken Sie auf „Submit“. Nach einiger Zeit erhalten Sie wichtige Informationen bzgl. der Sicherheit Ihrer Konfiguration!

Hier das Ergebnis des Tests der Konfiguration, die hier im Tutorial beschrieben ist (Stand 18.08.2015):




Assessed on: Tue, 18 Aug 2015 10:14:42 UTC | [Clear cache](#)

[Scan Anot](#)

### Summary

Overall Rating



Certificate	100
Protocol Support	95
Key Exchange	100
Cipher Strength	90

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS\_FALLBACK\_SCSV to prevent protocol downgrade attacks.