

# Erzeugung einer CSR (Certificate Signing Request) für IIS5, IIS6 und Apache

## CSR-Erzeugung für IIS5 und IIS6

Eine Zertifikatsanforderungsdatei (Certificate Signing Request File) in Microsoft IIS 5 und IIS 6 erstellen:

Der erste Schritt zum Erwerb eines Server-Zertifikats, ist das Erstellen der „Zertifikatsanforderungsdatei“. Für die Erstellung einer neuen „Zertifikatsanforderung“ führen Sie folgende Schritte durch:

1. Öffnen Sie den Internet Services Manager (oder Ihre Kunden MMC, die das IIS Plug-in beinhaltet). Diesen erreichen Sie über: **Start → Einstellungen → Systemsteuerung → Verwaltung → Internetdienste Manager**
2. Navigieren Sie zu der Seite, für die Sie eine sichere Kommunikation ermöglichen wollen.
3. Klicken Sie mit der rechten Maustaste auf den Namen der Website und gehen Sie auf „Eigenschaften“.
4. Klicken Sie auf die Registerkarte „Verzeichnissicherheit“.
5. Unter dem Abschnitt „Sichere Kommunikation“ klicken Sie auf „Server-Zertifikat“.
6. Damit starten Sie den neuen Web-Server-Zertifikat-Assistenten.
7. Klicken Sie auf „Weiter“.
8. Wählen Sie „Neues Zertifikat erstellen“ und klicken Sie auf „Weiter“ (Bevor das nächste Fenster erscheint, gibt es eine kurze Pause).
9. Wählen Sie die Option „Anforderung jetzt vorbereiten, aber später senden“ aus und klicken Sie auf „Weiter“.
10. Wählen Sie einen Anzeigenamen für die Seite. Dieser ist frei wählbar. Sie können zum Beispiel den Namen der Seite in der MMC wählen, oder den Namen des Kunden, dem die Webseite gehört.
11. Wählen Sie die Bit-Länge des Schlüssels, die Sie verwenden möchten. Klicken Sie die Option SGC an, wenn Sie Server Gated Cryptography verwenden wollen. Klicken Sie anschließend auf „Weiter“
12. Geben Sie Ihre Organisation (O) und Ihre Organisationseinheit (OU) ein. Klicken Sie dann auf „Weiter“.
13. Geben Sie den Common Name (CN) bzw. den Gemeinsamen Namen für Ihre Website ein. Dies sollte der DNS-Name Ihres Webservers sein.
14. Klicken Sie auf „Weiter“.
15. Geben Sie Ihr Land / Region, Stadt und Staat ein. Es ist sehr wichtig, dass Sie die Namen des Staates oder der Stadt nicht abkürzen. Wenn Sie fertig sind, klicken Sie auf „Weiter“.
16. Wählen Sie einen Namen für die Zertifikatsanforderungsdatei, die Sie gerade erstellen. Diese Datei enthält alle Informationen, die Sie hier erstellen, wie auch Ihren öffentlichen Schlüssel für Ihre Website. Wenn Sie mögen, können Sie Ihre Verzeichnisse nach dem Dateinamen durchsuchen. Haben Sie den Vorgang abgeschlossen, erhalten Sie eine txt-Datei. Der Standard-Name für die Datei ist Certreq.txt. Wenn Sie diesen Schritt abgeschlossen haben, klicken Sie auf „Weiter“.
17. Es werden Ihnen nun in einer zusammenfassenden Übersicht alle Informationen angezeigt, die Sie eingegeben haben. Stellen Sie sicher, dass alle diese Informationen korrekt sind. Klicken Sie anschließend auf „Weiter“.

18. Nun haben Sie Ihre Zertifikatsanforderungsdatei erstellt. Klicken Sie auf „Fertig stellen“ um die Requesterstellung abzuschließen.

# CSR-Erzeugung für Apache

Das Erstellen der Zertifikatsanforderungsdatei (Certificate Signing Request File) in Apache mod-SSL und BEN-SSL:

Das Dienstprogramm „OpenSSL“ wird benutzt, um sowohl den privaten Schlüssel als auch die Zertifikatsanforderung zu erstellen.

OpenSSL ist normalerweise unter /usr/local/ssl/bin installiert.

Wenn Sie eine individuelle Installation von openssl nutzen, müssen Sie diese Anweisungen dementsprechend anpassen.

Um einen privaten Schlüssel und den dazugehörigen öffentlichen Schlüssel für einen Webserver „myserver“ zu erstellen, verwenden Sie den folgenden Befehl:

```
openssl req -new -nodes -keyout myserver.key -out myserver.csr
```

Es werden zwei Dateien erstellt (es werden Ihnen einige Fragen gestellt, siehe unten). Die Datei myserver.key beinhaltet einen privaten Schlüssel, diesen niemals für irgendjemanden offenlegen. Schützen Sie den privaten Schlüssel sorgfältig.

Insbesondere muss eine Sicherungskopie vom privaten Schlüssel erstellt werden, denn man kann diesen niemals wiederherstellen, wenn er jemals verloren gehen sollte. Der private Schlüssel wird zur Erstellung einer Zertifikatsanforderungsdatei benötigt.

Sie müssen nun die Informationen eingeben, die in Ihrem Antrag für ein Zertifikat benötigt werden.

Was Sie im Folgenden eingeben, wird als Distinguished Name oder DN bezeichnet.

Es gibt zahlreiche Felder auszufüllen, aber Sie können auch einige leer lassen.

Für einige Bereiche gibt es einen Standard-Wert.

Wenn Sie "." eingeben, wird das Feld leer gelassen.

Country Name (2 letter code) (**Land (2 Buchstaben Code)**) [AU]: de

State or Province Name (full name) [Some-State] (**Staat oder Provinz Name (ausgeschrieben)**): Berlin

Locality Name (eg, city) (**Veranstaltungsort Name (das ist: Stadt)**): Berlin

Organization Name (eg, company) [Internet Widgits Pty Ltd] (**Name der Organisation (die Firma)**): Meine Organisation

Organizational Unit Name (eg, section) (**Name der Firmenabteilung**): System Administration

Common Name (eg, YOUR name) (**Gebräuchlicher Name (das ist: Dein name)**): meinserver.meinedomain.de

Email Address (**Email Adresse**):

Please enter the following “extra“ attributes to be sent with your certificate request (**Bitte geben Sie folgende "extra"-Attribute ein, welche dann mit Ihrem Antrag für ein Zertifikat verwendet werden sollen**):

A challenge password (**Ein sicheres Passwort**):

An optional company name (**Ein optionaler Firmenname**):

Use the name of the webserver as Common Name (CN). If the domain name is „mydomain.de“ append the domain to the hostname (use the fully qualified hostname).

**(Verwenden Sie den Namen des Webservers als Common Name (CN) bzw. Gemeinsamen Namen. Wenn der Domain-Name "mydomain.de" ist, hängen Sie die Domain auf den Hostnamen an (verwenden Sie den vollständig qualifizierten Hostnamen).)**

The fields „email address“, „optional company name“ and „challenge password“ can be left blank for a webserver certificate.

**(Die Felder "E-Mail-Adresse", "optionaler Firmenname" und "sicheres Passwort" können für ein Webserver-Zertifikat leer gelassen werden.)**