FileMaker Server mit selbstsigniertem SSL-Zertifikat ausstatten

Es ist möglich in Filemaker Server ein selbstsigniertes Zertifikat zu verwenden.

Filemaker erkennt dieses Zertifikat nicht als „gültig“ an, da es nicht bei Filemaker gelistet ist. Dies hat aber rein gar nichts mit der technischen Sicherheit eines SSL-Zertifikats zu tun.

Wem kann man am aller besten vertrauen? – sich selbst.

Damit ein SSL-Zertifikat in Filemaker mit einem „grünen“ Schloss gekennzeichnet wird, muss es von einer von Filemaker anerkannten Zertifizierungsstelle stammen.

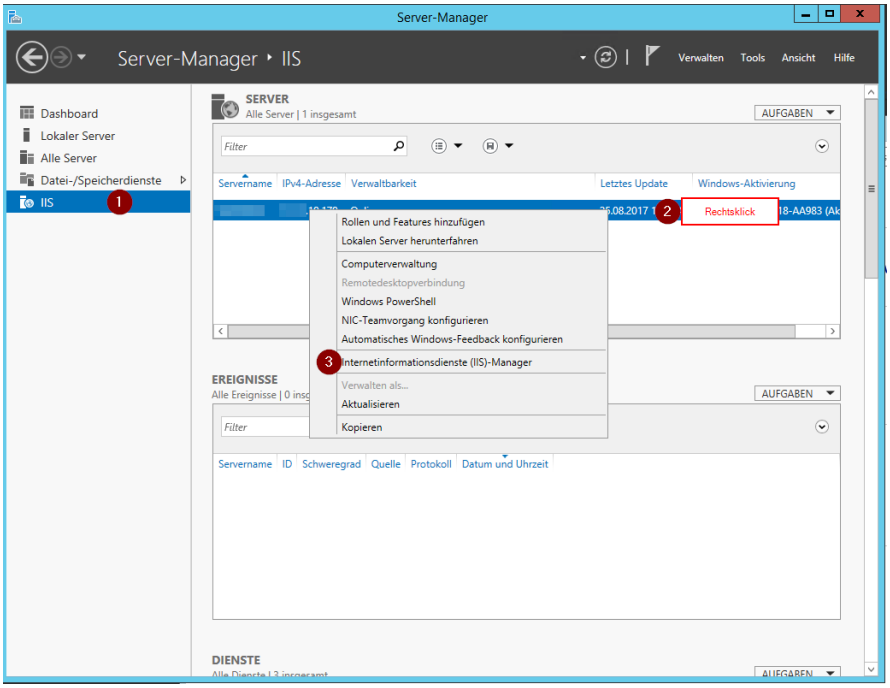
Diese SSL-Zertifikate sind aber kostenpflichtig und das nicht immer günstig.

Filemaker Server hat ein SSL-Zertifikat bereits inkludiert, jedoch darf man dies lt. Filemaker Lizenzvereinbarung nur für Testzwecke nutzen. Sollte ich nun an meinen Datenbanken nichts testen, verstoße ich eigentlich gegen die Vereinbarung.

Wir erstellen deshalb ein selbstsigniertes SSL-Zertifikat mittels eines Windows Server 2012 R2 Datacenter.

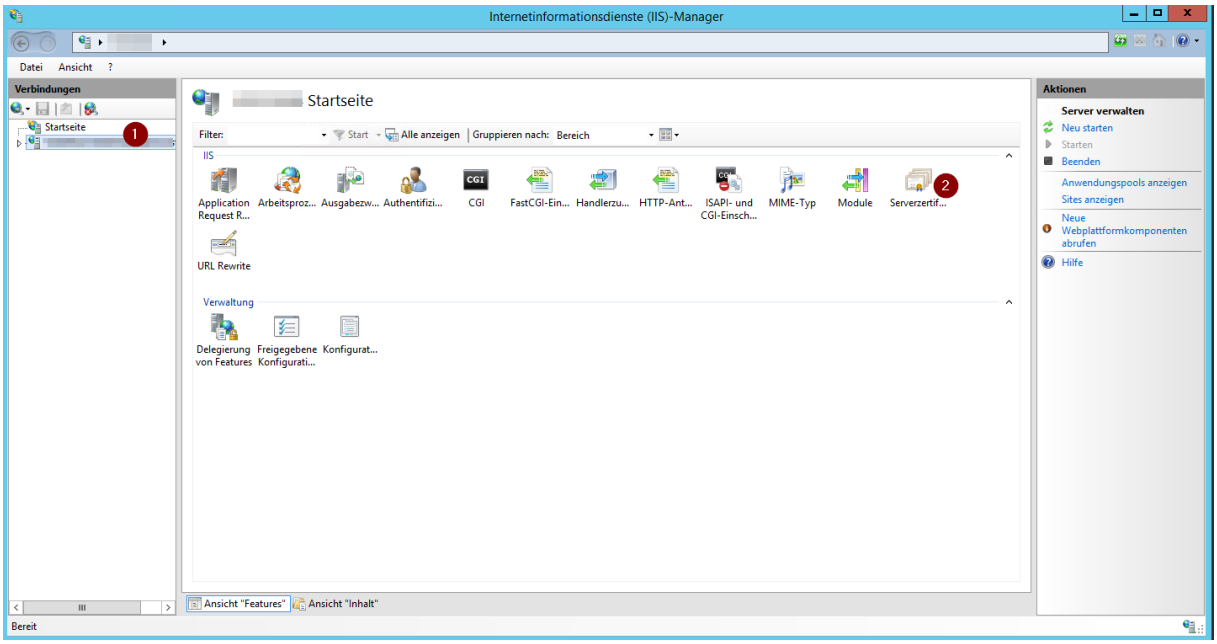
Schritt 1

- Starten Sie den Server-Manager
- Navigieren Sie zu IIS, links im Menu
- Markieren Sie den gewünschten Server und klicken mit der rechten Maustaste
- Wählen Sie im Menü -> „Internetinformationsdienste (IIS)-Manager“



Schritt 2

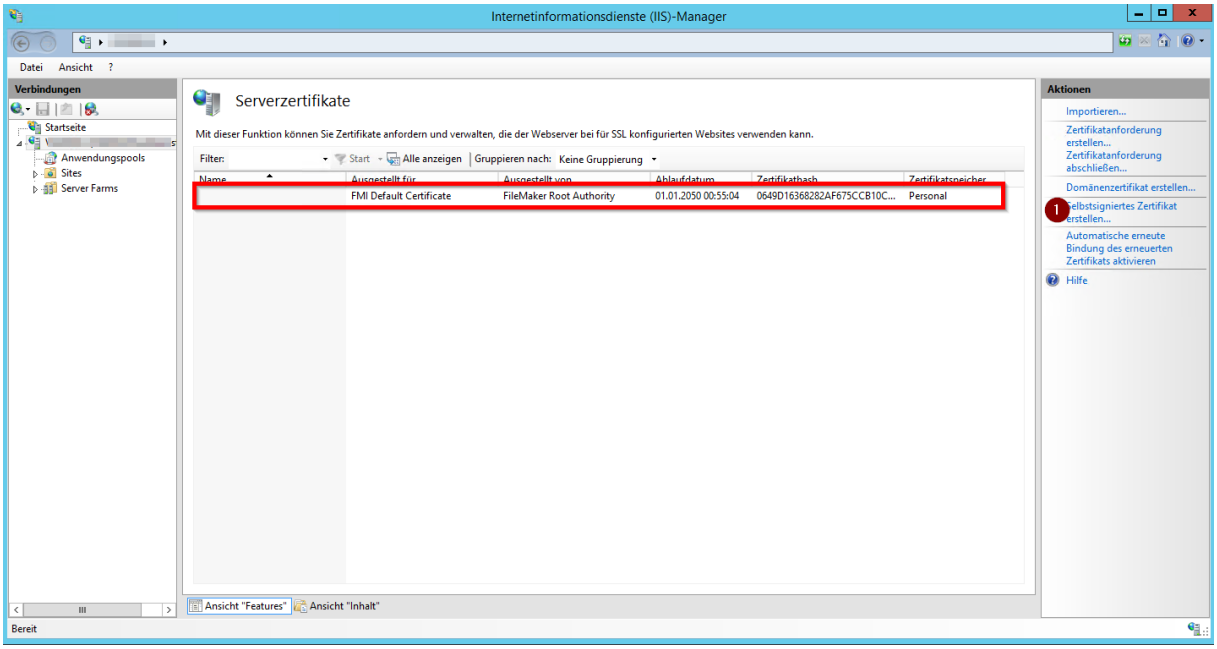
- Wählen Sie Ihren Anwendungspool
- Doppelklicken Sie auf Serverzertifikate



Schritt 3

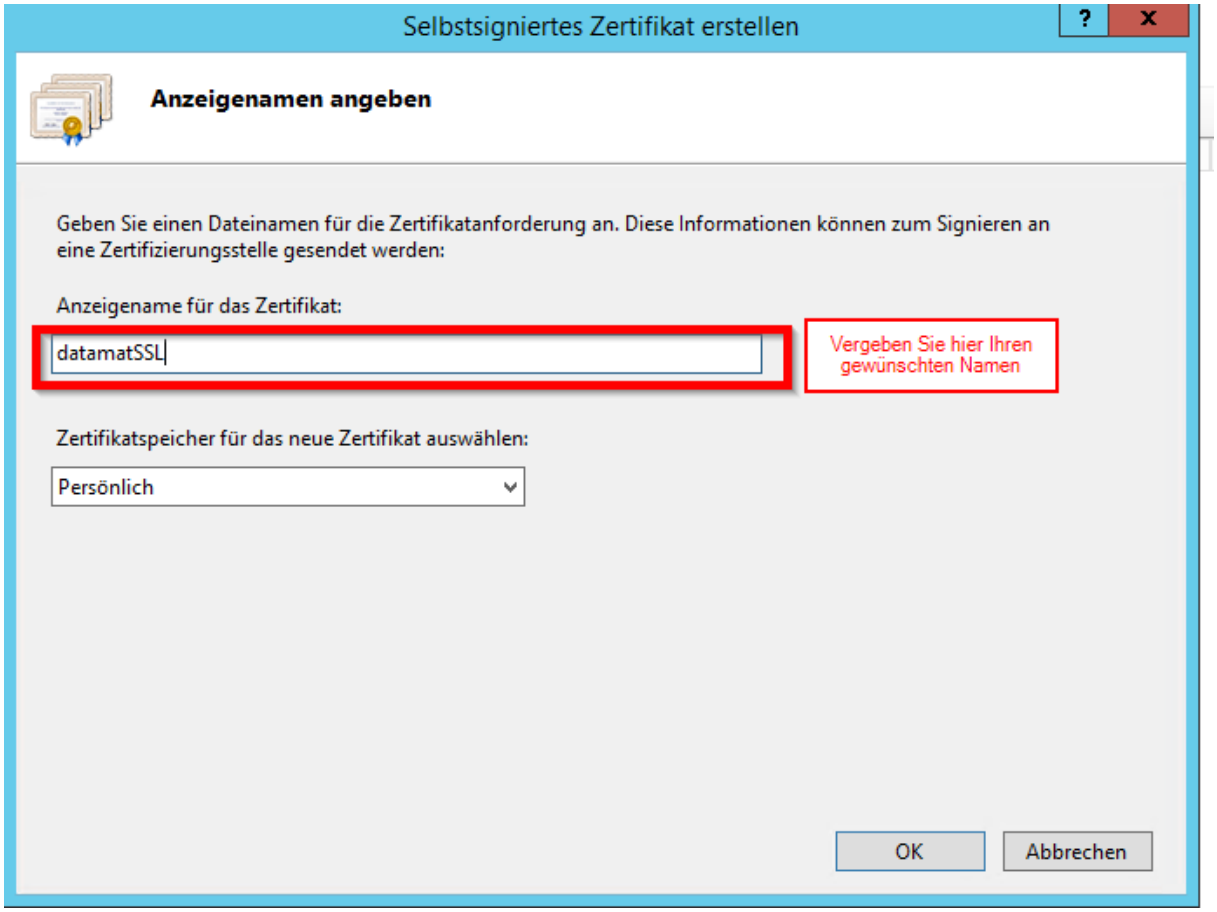
Hier sehen Sie u.a. das FileMaker-Zertifikat, das sich bei der Installation von FileMaker Server mitinstalliert.

- Klicken Sie rechts auf „Selbstsigniertes Zertifikat erstellen…“



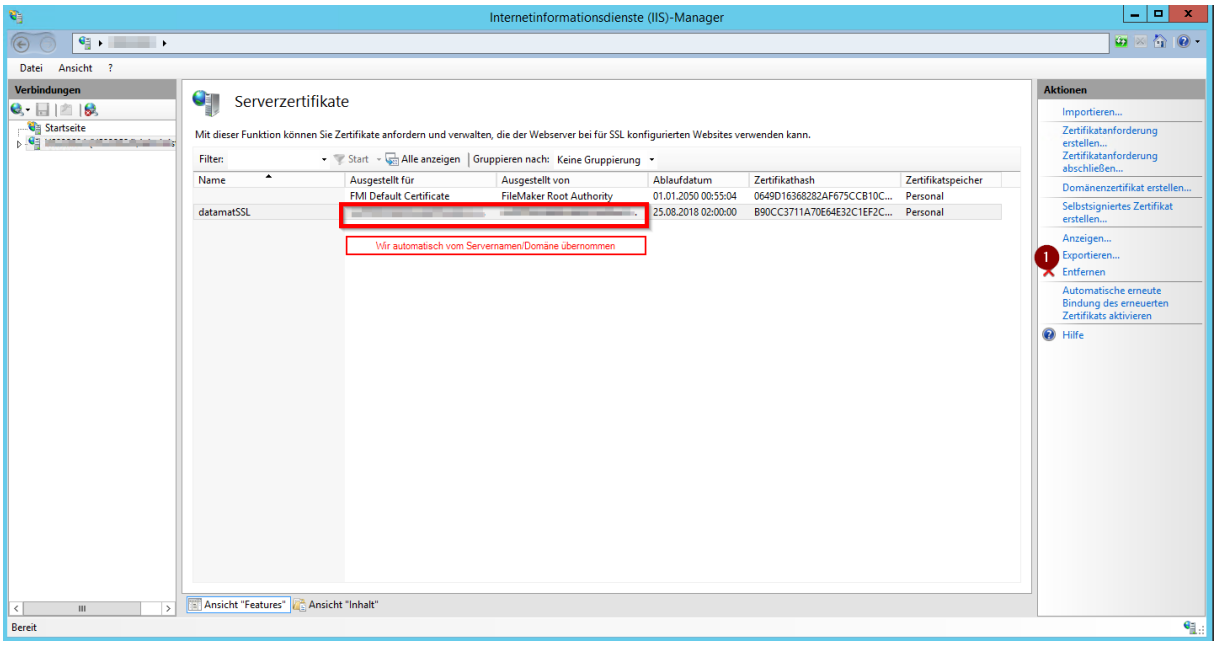
Schritt 4

- Vergeben Sie einen Namen für das Zertifikat
- Stellen Sie den Zertifikatsspeicher auf „persönlich“
- Klicken Sie auf „ok“

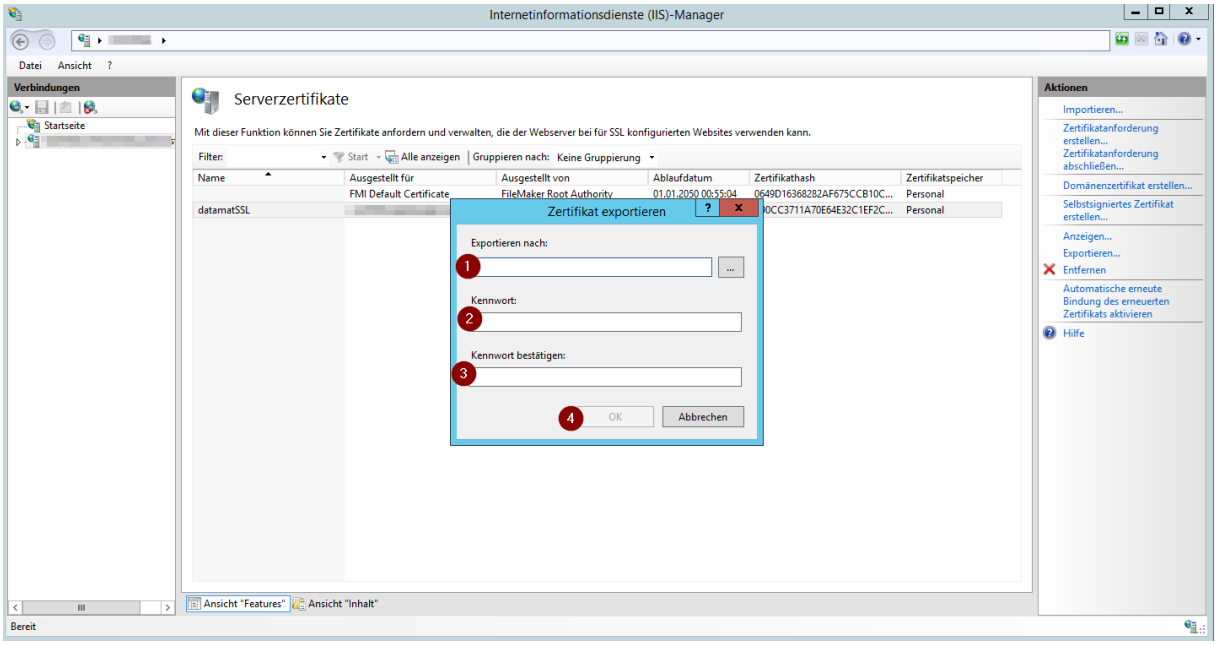


Schritt 5

Nach Erstellung finden Sie das eben erstellte Zertifikat in der Liste.



- Markieren Sie dieses Zertifikat
- Klicken Sie rechts auf exportieren

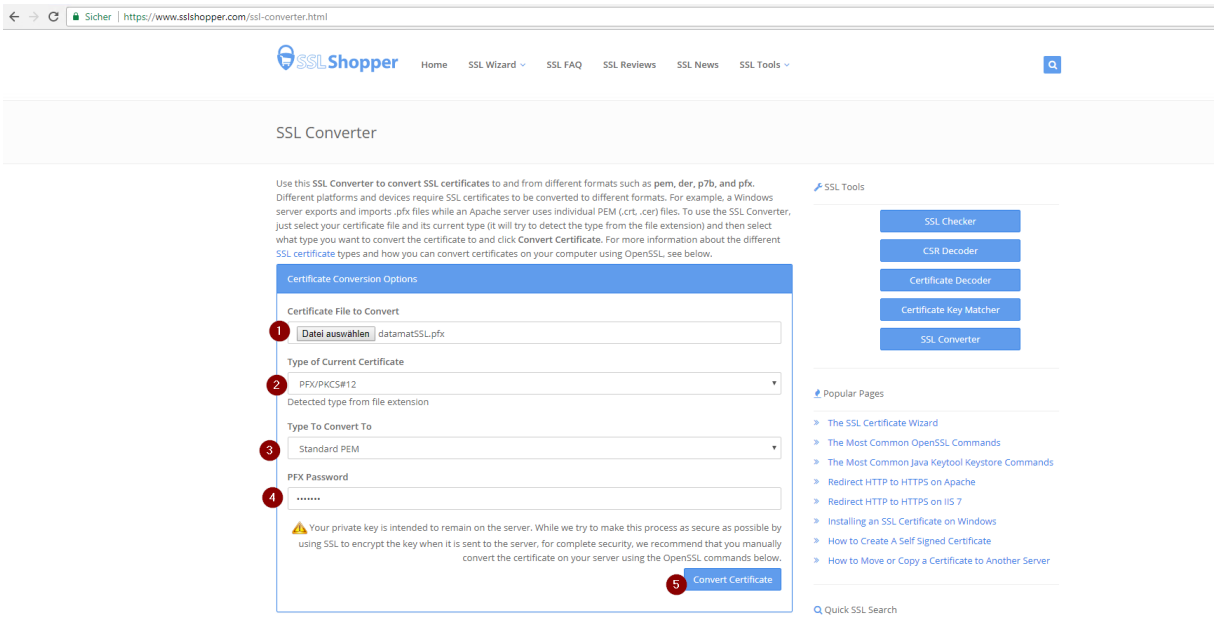


- Wählen Sie einen Speicherort und ein Passwort

Schritt 6

Windows erzeugt Zertifikatsdateien mit der Endung „pfx“. Diese Dateiendung kann aber nicht als Zertifikat für FM Server verwendet werden. Die pfx-Datei muss in eine pem-Datei umgewandelt werden.

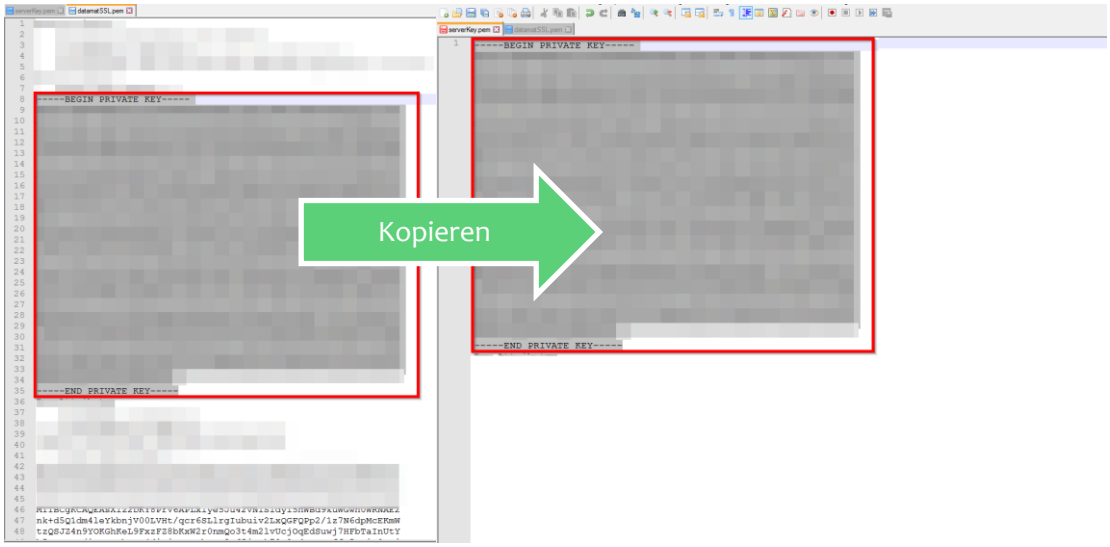
- Öffnen Sie einen Browser und gehen zu https://www.sslshopper.com/ssl-converter.html
- Wählen Sie die eben erstellte pfx-Datei aus
- Wählen Sie als Type of Current Certificate „PFX/PKCS#12“
- Wählen Sie als Type To Convert To „Standard PEM“
- Geben Sie in PFX Password das Passwort auf Schritt 5 an
- Klicken Sie Convert Certificate
- Speichern Sie das pem-File an beliebigem Ort



Schritt 6

Beim Import überprüft FileMaker-Server, ob in der „serverKey.pem“ der private Key zum importierenden Zertifikat vorhanden ist. Diese Datei muss nun händisch bearbeitet werden.

- Navigieren Sie zu dem Filemaker-Server-Ordner „CStore“
- C:\Program Files\FileMaker\FileMaker Server\CStore
- Öffnen Sie die Datei serverKey.pem, oder erstellen Sie sie
- Öffnen Sie die konvertierte pem-Datei aus Schritt 6
- Kopieren Sie aus der konvertierten pem-Datei als von
  ----BEGIN PRIVATE KEY ----- bis
  ----- END PRIVATE KEY-----
- Fügen Sie diesen kopierten Inhalt in die serverKey.pem ein
- Speichern Sie die Dateien



Schritt 7

Der FileMaker-Server ist über die Console/Power Shell sehr einfach für den Import der Datei zu administrieren.

- Starten Sie die Console/Power Shell mit Adminrechten
- Geben Sie dieses Kommando ein: *fmsadmin certificate import PfadZumPEM*
- Drücken Sie die Return/Eingabetaste

Schritt 8

Starten Sie Filemaker-Server neu.

- Starten Sie die Console/Power Shell
- Geben Sie dieses Kommando ein: *fmsadmin restart server*
- Geben Sie „y“ ein
- Drücken Sie die Return/Eingabetaste
- Geben Sie den Benutzername für die Adminconsole ein
- Drücken Sie die Return/Eingabetaste
- Geben Sie das Passwort für Adminconsole ein
- Drücken Sie die Return/Eingabetaste

```
PS C:\Users\Administrator> fmsadmin restart server
C:\Program Files\FileMaker\FileMaker Server\Database Server\fmsadmin.exe: really restart server? (y, n) y
username (Administrator):admin
password:********
PS C:\Users\Administrator> _
```

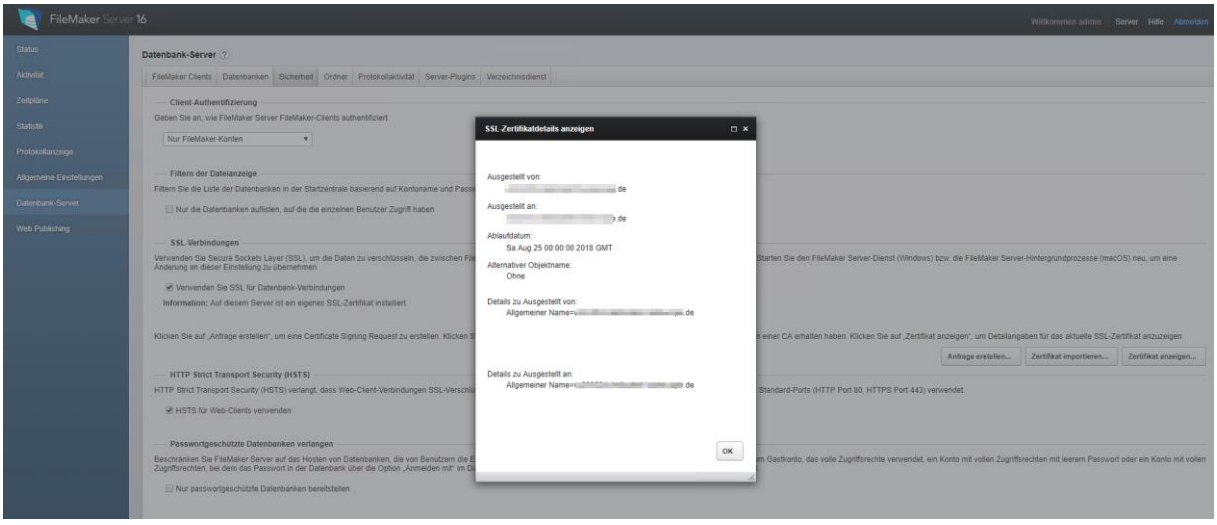
Dieser Vorgang dauert etwa 3 Minuten.

Schritt 9

Falls Sie SSL noch nicht im FileMaker Server aktiviert haben, aktvieren Sie SSL.

Prüfen Sie, ob das SSL-Zertifikat korrekt installiert ist.

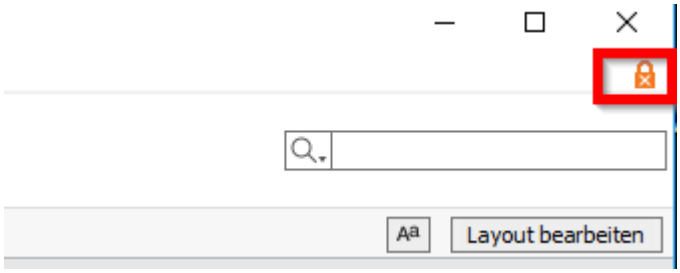
- Loggen Sie sich in Filemaker Server ein
- Gehen Sie zu Datenbank-Server
- Auf den Reiter „Sicherheit“
- Zertifikat anzeigen



Schritt 10

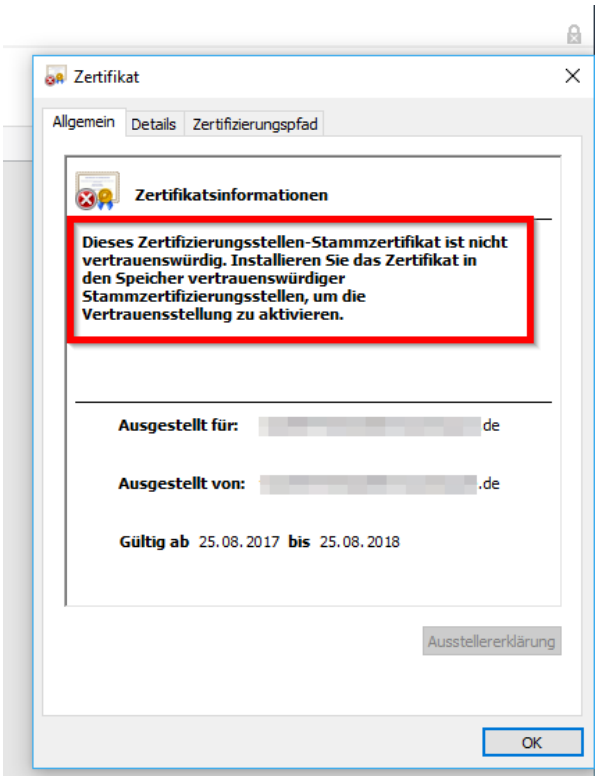
Stellen Sie Verbindung mittels FileMaker Pro zum FileMaker Server her.

- Klicken Sie oben rechts auf das Schlosssymbol und lassen sich die Informationen zum Zertifikat anzeigen



Sie sehen nun das Zertifikat und können nochmals prüfen, ob alles korrekt ist.

Es erscheint zu dem eine Zertifikatswarnung.



Das liegt daran, dass das Zertifikat Ihrem PC noch nicht bekannt/vertrauenswürdig ist.

Sie sind bereits per selbstsigniertem Zertifikat verbunden, wenn Sie wollen, dass das Zertifikat für gültig erklärt wird fahren Sie mit den weiteren Punkten fort.

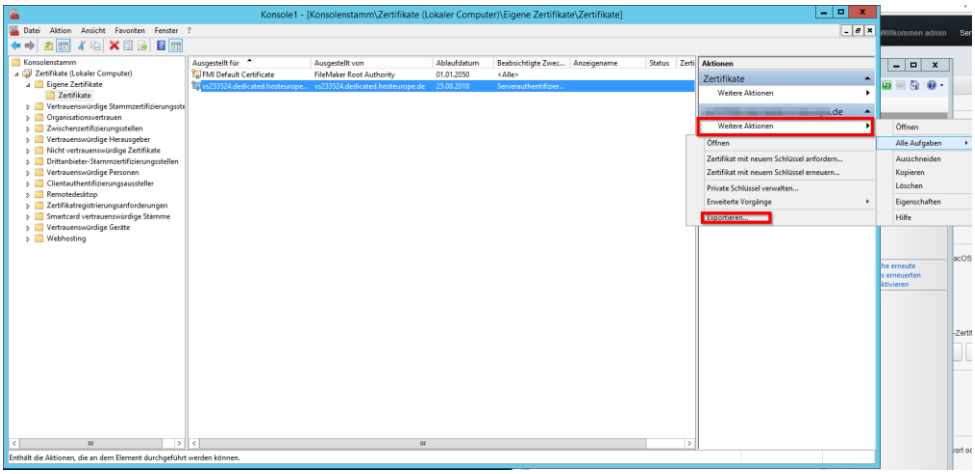
Schritt 11

Damit das Zertifikat von Ihrem PC als gültig eingestuft wird, muss dieses in jedem Client der auf den Filemaker-Server zugreifen möchten hinterlegt werden.

- Öffnen sie auf Ihrem Windows Server 2012 die Console/Power Shell als Administrator
- Geben Sie diesen Befehl ein: *mmc*
- Drücken Sie die Return/Eingabetaste
- Es öffnet sich eine Konsole
- Klicken Sie dort auf Datei-> Snap-In hinzufügen/entfernen (STRG+M)
- Wählen Sie links im Menü „Zertifikate“
- Klicken Sie auf hinzufügen
- Wählen Sie „Computerkonto“
- Klicken Sie „weiter“
- Belassen Sie die Einstellung auf „Lokalen Computer“ und klicken „fertig stellen“
- Klicken Sie „ok“

Nun ist links ein Punkt „Zertifikate (Lokaler Computer) aufgetaucht.

- Öffnen Sie die Baumstruktur diesen Punktes
- Wählen Sie Eigene Zertifikate->Zertifikate
- Wählen Sie das eigene Zertifikat aus
- Drücken Sie die Return/Eingabetaste



- Klicken Sie rechts auf „Weitere Aktionen“
- Alle Aufgaben
- Exportieren
- Klicken Sie auf „weiter“
- Wählen Sie „Nein, privaten Schlüssel nicht exportieren“
- Klicken Sie auf „weiter“
- Wählen Sie DER-codiert-binär X.509 (.CER)
- Klicken Sie auf „weiter“
- Speichern Sie es an einem beliebigen Ort
- Klicken Sie auf „weiter“
- Klicken Sie „Fertig stellen“

Schritt 12

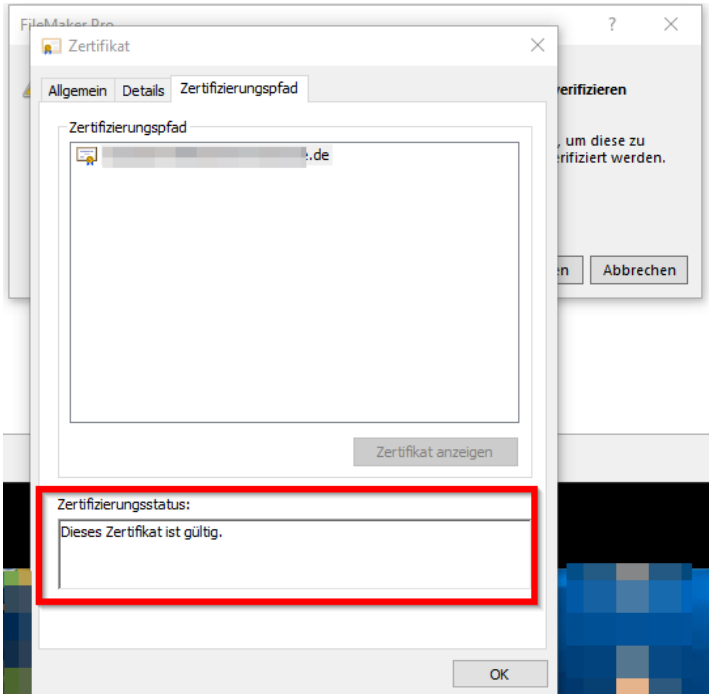
Das in Schritt 11 erstellte cer-File muss nun auf jedem Rechner installiert werden.

- Kopieren Sie das cer-File aus Schritt 10 auf den Client-PC
- Öffnen Sie am Client-PC die Console/Power Shell als Admin
- Geben Sie diesen Befehl ein: *mmc*
- Drücken Sie die Return/Eingabetaste
- Es öffnet sich eine Konsole
- Klicken Sie dort auf Datei-> Snap-In hinzufügen/entfernen (STRG+M)
- Wählen Sie links im Menü „Zertifikate“
- Klicken Sie auf hinzufügen
- Wählen Sie „Computerkonto“
- Klicken Sie „weiter“
- Belassen Sie die Einstellung auf „Lokalen Computer“ und klicken „fertig stellen“
- Klicken Sie „ok“

Nun ist links ein Punkt „Zertifikate (Lokaler Computer) aufgetaucht.

- Öffnen Sie die Baumstruktur diesen Punktes
- Wählen Sie Vertrauenswürdige Stammzertifizierungsstellen->Zertifikate
- Klicken Sie rechts auf „Weitere Aktionen“
- Alle Aufgaben
- Importieren
- Wählen Sie „Lokaler Computer“
- Klicken Sie „weiter“
- Geben Sie den Speicherort der in Schritt 11 erstellten Datei an
- Klicken Sie „weiter“
- Wählen Sie „Alle Zertifikaten in folgendem Speicher speichern“
- Geben Sie als Zertifikatsspeicher an: *Vertrauenswürdige Stammzertifizierungsstellen*
- Klicken Sie „weiter“
- Klicken Sie „Fertig stellen“

Wird nun Filemaker neugestartet und man betrachtet das Zertifikat ist dieses wie im Gegensatz zu Schritt 10 nun gültig.



Ein selbstsigniertes Zertifikat wird wahrscheinlich niemals „grün“ gekennzeichnet. Ein selbstsigniertes SSL-Zertifikat bietet technisch die gleiche Sicherheit wie ein gekauftes.

Diese Anleitung wurde erstellt von:

Alexander Baier – datamat Software Development
Kohplatzstr. 15
78628 Rottweil
support@datamat.software