Wie kann ich überprüfen, ob mein privater Schlüssel zu meinem Zertifikat passt?

Die folgenden Hinweise sind der Apache FAQ entnommen.
http://httpd.apache.org/docs/2.0/ssl/ssl_faq.html#verify

Für die Beispiele in diesem Artikel nehmen wir folgendes an:

- *server.pem sei das angelieferte Server-Zertifikat*
- *server.key sei die Datei mit Ihrem Schlüsselpaar*
- *server.csr sei die Datei mit dem Zertifikatsantrag (CSR)*

Eine private Schlüsseldatei enthält im wesentlichen den „public key“ und den „private key“. Die „public key“-Bits werden beim erzeugen eines CSR verwendet und sind dann anschließend Teil des zugehörigen Zertifikates.

Um zu überprüfen, ob der öffentliche Schlüssel in Ihrem Zertifikat mit dem öffentlichen Teil Ihres Schlüsselpaares übereinstimmt, müssen Sie einfach diese Zahlen vergleichen. Mit den folgenden openSSL-Kommandos zeigen Sie den Inhalt der entsprechenden Dateien:

```
openssl x509 -noout -text -in server.pem
openssl rsa -noout -text -in server.key
```

Beispiel (Auszug aus der Ausgabe von openssl):

```
Modulus (2048 bit):
    00:b8:d6:e9:a9:ff:ea:0b:f6:05:bf:bf:c9:2f:b6:
    da:13:9c:1f:de:50:82:de:53:54:61:ef:32:bd:3c:
    5f:ce:3f:b8:0a:67:d6:98:38:4b:ad:ef:0c:bc:cc:
    e8:e2:d6:90:87:2a:6f:9b:17:c0:18:78:e0:67:84:
    5c:dd:f6:8d:41:cc:ad:25:47:99:92:df:84:e8:57:
    70:c2:7c:c2:f4:30:aa:e1:5e:75:00:a7:bd:6d:33:
    f7:ec:9f:55:c0:66:5f:40:f7:36:61:cb:ae:30:4e:
    41:48:80:22:93:00:0f:42:0d:3a:8c:6b:2d:9d:07:
    e9:a4:7c:c1:29:34:cd:c5:70:0d:a3:b4:fd:7e:43:
    9a:05:b0:1a:bb:ab:95:6f:5a:95:88:77:14:21:b8:
    b8:bf:f8:82:09:f0:9c:11:6b:25:b5:5c:72:6a:fd:
    62:a8:1e:d8:fc:c2:80:83:2e:e4:7a:b7:f2:79:fc:
    cc:45:83:cb:9c:ae:5d:9f:32:27:d6:ba:39:5d:29:
    fa:2b:30:ad:b2:81:1c:23:8d:28:25:b9:5c:ce:cd:
    ff:45:84:a9:7f:55:82:4b:2e:26:7e:c6:a6:d7:9d:
    5c:a5:93:a6:0e:d6:23:de:41:ee:51:16:27:c6:15:
    f7:a4:b6:68:83:94:b0:da:ea:95:8c:1b:1a:b4:bb:
    cd:69
```

```
Exponent: 65537 (0x10001)
```

Die Teile „Modulus“ und „Exponent“ der beiden Dateien müssen übereinstimmen.

Der Exponent ist eine relativ kleine Zahl, die ohne Probleme verglichen werden kann.

Es ist allerdings schwierig, visuell zu überprüfen, ob die langen Modulus-Zahlen gleich sind. Zur Abhilfe können Sie die beiden Modulus-Werte aus den Dateien extrahieren lassen und sie anschließend als md5-Hash ausgeben. Diese kürzeren Zahlen lassen sich visuell leichter vergleichen.

```
openssl x509 -noout -modulus -in server.pem | openssl md5
openssl rsa -noout -modulus -in server.key | openssl md5
```

Beispiel:

```
5dd0e29d5b90309f51479a60b2f1edce
```

Es ist zwar theoretisch möglich, daß diese Zahlen identisch sind, obwohl die Modulus-Werte sich unterscheiden, aber die Wahrscheinlichkeit hierfür ist extrem gering.

Es bleibt Ihnen natürlich unbenommen, die beiden langen Modulus-Werte in Dateien zu speichern und dann die Dateien mit Hilfe eines Programmes zu vergleichen.

Falls Sie prüfen wollen, zu welchem Schlüssel oder Zertifikat eine bestimmte CSR gehört, können Sie dieselbe Berechnung auf die CSR anwenden:

```
openssl req -noout -modulus -in server.csr | openssl md5
```

Zertifikate - Artikelübersicht, Sicherheit - Artikelübersicht