# Beantragung von digitalen Zertifikaten an der Frankfurt UAS

## Inhaltsverzeichnis




**Ähnliche Artikel**

- Beantragung von digitalen Zertifikaten an der Frankfurt UAS


Einstiegspunkt für eine Beantragung ist

https://pki.pca.dfn.de/fh-ffm-ca-g2/pub

Über Reiter wird gewählt, ob ein Nutzerzertifikat oder ein Serverzertifikat beantragt werden soll.

## Nutzerzertifikat

Die Beantragung des Nutzerzertifikats erfolgt vollständig geführt über die Web-GUI und sollte selbsterklärend sein. Am Ende kann über einen Button der Zertifikatsantrag heruntergeladen werden, der ausgefüllt und unterschrieben perönlich dem Service Desk zur Prüfung vorzulegen ist. Die Übermittlung des Zertifikats erfolgt dann nach Genehmigung an die im Beantragungsprozess angegebene E-Mail Adresse.

**Bitte beachten: Die JSON-Datei, die Sie bei Antragsstellung am Ende herunterladen können, bitte gut aufbewahren. Diese wird benötigt um das Zertifikat abholen zu können.**

## Serverzertifikat

Auch die Beantragung eines Serverzertifikats erfolgt geführt über die Web-GUI und sollte selbsterklärend sein. Wenn gewünscht, so kann auch eine Beantragung über die Vorab-Erstellung eines Zertifikatsantrags im PKCS#10-Format (Format eines CSRs - Certficate Signign Request) erfolgen. Eine Anleitung hierzu findet sich weiter unten.

Am Ende den Zertifikatsantrag herunterladen, ausfüllen und unterschrieben dem Service Desk persönlich zur Prüfung vorlegen. Die Übermittlung des Zertifikats erfolgt dann an die im Beantragungsprozess angegebene E-Mail Adresse.

**Bitte beachten: Die JSON-Datei, die Sie bei Antragsstellung am Ende herunterladen können, bitte gut aufbewahren. Diese wird benötigt um das Zertifikat abholen zu können.**

## Serverzertifikat abholen

Sobald das Zertifikat genehmigt wurde und Sie die Mail dazu erhalten können Sie ihr Zertifikat abholen. Hierzu folgen bitte dem Link folgen: https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/1450/certificates

Hier wird zuerst die JSON-Datei hochgeladen und im Anschluss kann das Zertifikatspaket heruntergeladen werden. Dies beinhaltet: Zertifikat, Chain (Zwischenzertifikate) und den privaten Schlüssel. Das Ganze steht im PKCS12-Format bereit, was man an der Endung .p12 erkennen kann. Nicht alle Server "wollen" dieses Format, daher können hier noch weitere Schritte notwendig sein, die im Anschluss erläutert werden.

### Zertifikat (mit Chain) und privaten Schlüssel extrahieren

Mittel der Wahl ist das Tool *openssl*.

```
openssl pkcs12 -in <Zertifkatsdatei>.p12 -out <Zertfikatsdatei>.pem -nodes
```

Wird ein *-nocerts* angehängt, so erhält man nur den privaten Schlüssel, mit einem *-nokeys* nur das Zertifikat mit Chain.

Wird nur das Zertifikat ohne Chain benötigt, gibt es 2 Möglichkeiten.

1. In der Mail vom DFN ist das Zertifikat ohne Chain angehängt und kann verwendet werden
2. unter Linux/Mac: mit Beispielsweise dem Tool vi wird die Datei bearbeitet und die Chain entfernt

#### Passwort vom Schlüssel entfernen

**Achtung: Grundsätzlich sollte ein private Key immer mit einem Passwort gesichert werden, um ihn vor unberechtigten Zugriffen zu schützen!** Manche Applikation fordern jedoch einen Schlüssel ohne Passwort. Dieses kann wie folgt entfernt werden:

```
openssl rsa -in <server>_key.pem -out new<server>_key.pem
```

## Zertifikatsantrag im PKCS#10-Format erstellen

Mittel der Wahl zur Erstellung eines solchen Antrags ist das Kommandozeilenwerkzeug *openssl* aus der gleichnamigen Software zur Transportverschlüsselung. Das Programm erlaubt die Beantragung, Erzeugung und Verwaltung von Zertifikaten und ist Bestandteil gängiger Linux-Distributionen. Die Erstellung kann, muss aber nicht auf dem Rechner erfolgen, für den das Zertifikat beantragt wird.

> **Hinweis: Installation unter Windows**
>
> Eine Möglichkeit, *openssl* auch unter Windows nutzen zu können, ist Git for Windows, das neben weiteren Werkzeugen auch *openssl.exe* und eine BASH Emulation als Kommandozeile bereit hält. Innerhalb dieser Umgebung lassen sich die weiteren Anweisungen auch unter Windows ausführen.

### Erster Schritt: Schlüssel (key) generieren, mit dem der Antrag signiert wird

```
openssl genrsa -out <server>_key.pem 2048
```

Die Datei <server>_key.pem (*bitte den eigenen Anforderungen anpassen!)* enthält den privaten und öffentlichen Schlüssel und wird mit einem Passwort geschützt. Da die angestrebte Sicherheit der Datenkommunikation von diesem Schlüssel abhängt, sollte er sicher aufbewahrt und das Passwort hinreichend komplex gewählt werden.

In bestimmten Fällen kann es notwendig sein, den Schlüssel ohne Passwort bereitzustellen. Das Passwort kann jederzeit entfernt werden:

```
openssl rsa -in <server>_key.pem -out <server>_key_nopw.pem
```

Der Schlüssel muss in diesem Fall aber mit anderen Mitteln adäquat geschützt werden.

### Zweiter Schritt: Antrag erstellen

```
openssl req -batch -sha256 -new -key <server>_key.pem
            -out <server>_req.pem
            -subj '/C=DE/ST=Hessen/L=Frankfurt am Main
                   /O=Frankfurt University of Applied Sciences
                   /OU=<Abteilung>/CN=<server>.<subdomain>.frankfurt-university.de
                   /emailAddress=<mailadresse>@<subdomain>.fra-uas.de'
```

Die obige Sequenz muss ***angepasst*** und ***am Stück in einer Zeile*** eingegeben werden.

Das Ergebnis <server>_req.pem kann vor Übermittlung nocheinmal geprüft werden:

```
openssl req -in <server>_req.pem -noout -text
```

Anschließend den Antrag über den entsprechenden Formularpunkt hochladen und den Antragsprozess in der GUI abschließen. Am Ende den Zertifikatsantrag herunterladen, ausfüllen und unterschrieben dem Service Desk persönlich zur Prüfung vorlegen. Die Übermittlung des Zertifikats erfolgt dann an die im Beantragungsprozess angegebene E-Mail Adresse.

### PFX/PKCS#12-Datei erstellen

In bestimmten Fällen ist es erforderlich, dass das Zertifikat als **PKCS#12-Datei** vorliegt. Solche Dateien fassen die erforderlichen Bestandteile in einer einzigen Datei zusammen. Es müssen vorliegen:

- RSA-Key: <server>_key.pem (wie oben erstellt)
- Zertifikat der DFN-PKI: <server>_crt.pem (kommt vom DFN als Mailanhang)
- CA-Zertifikatskette: komplette Vertrauenskette von der DFN-CA bis zur T-Systems CA. Diese Datei kann vom DFN bezogen werden:

```
wget https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt
```

Für die Erstellung wird wieder openssl verwendet:

```
openssl pkcs12 -export -inkey <server>_key.pem
               -in <server>_crt.pem
               -certfile chain.txt -out pkcs12 <server>.p12
```

Auch hier: alles in einer Zeile und Werte entsprechend anpassen!

### Die wichtigsten OpenSSL-Befehle in einer Übersicht:

https://help.internetx.com/display/SSL/OpenSSL+-+Die+wichtigsten+Befehle