

Serverzertifikat beantragen

Ein Serverzertifikat besteht aus einem privaten und einem öffentlichen Schlüssel, die mittels asymmetrischer Kryptographie zueinander passen. Der öffentliche Schlüssel, zusammen mit Metainformationen, wie dem Domainnamen, für den das Schlüsselpaar gültig ist, werden in einem *Certificate Signing Request* verpackt und durch die DFN PKI signiert. Das Resultat ist ein *öffentliches Serverzertifikat*, das ausschließlich mit dem *privaten Schlüssel* verwendet werden kann.

Speichern Sie den privaten Schlüssel nur auf Ihrem Server und erzeugen Sie ein Backup an einem sicheren Ort. Geben Sie den privaten Schlüssel niemals weiter und informieren Sie umgehend das Rechenzentrum, falls Sie den Schlüssel verlieren oder Grund zu der Annahme haben, dass dieser entwendet wurde!

Durch die Beantragung eines Server-Zertifikates sind Sie verpflichtet, die Regelungen und Pflichten von Zertifikatsinhabern in der DFN-PKI zu befolgen. Diese finden Sie unter <https://www.pki.dfn.de/fileadmin/PKI/Info-fuer-Zertifikatinhaber.pdf>.

Schlüsselpaar und Certificate Signing Request erstellen

Zur Beantragung eines Serverzertifikats sind zunächst dessen Bestandteile (Schlüsselpaar und Metainformationen) zu generieren. Dies kann mit OpenSSL, das praktisch für alle aktuellen Betriebssysteme verfügbar ist, geschehen. Wenn Sie GNU/Linux verwenden, steht Ihnen OpenSSL in aller Regel über den Paketmanager zur Verfügung. Unter Windows können Sie [WinOpenSSL](#) verwenden.

Konfigurationsdatei

Um das Schlüsselpaar und den Certificate Signing Request zu erstellen, verwenden Sie bitte die

Konfigurationsdatei der HS Fulda

. An dieser Konfigurationsdatei müssen Sie keine Änderungen vornehmen - es sei denn, Sie möchten das Zertifikat mit mehr als nur einem Namen. In diesem Fall geschieht eine Änderung ausschließlich in den Zeilen 46-50!

Schlüsselpaar und Certificate Signing Request

Geben Sie nun an der Kommandozeile folgendes Kommando ein, um das Schlüsselpaar zu erzeugen.

```
openssl req -new -nodes -out server.csr -keyout server.key -config  
openssl.cnf
```

Nun werden alle notwendigen Metainformationen abgefragt. Die meisten Informationen dürfen nicht verändert werden. Die Angabe der Abteilung (Organizational Unit Name) ist optional. Unter *Common name* geben Sie bitte den primären Servernamen ein.

Die Bestandteile, die in diesem Schritt generiert werden sind:

- Certificate Signing Request (Datei server.csr, zum Hochladen auf die Antrags-Webseite der DFN PKI)
- Privater Schlüssel des Server-Zertifikats (Datei server.key)

Zertifikatantrag stellen

Die Beantragung des Zertifikats erfolgt nun über das [Webportal des DFN-Vereins](#). Füllen Sie bitte das Formular aus mit Ihren Angaben aus und wählen Sie die zuvor erstellte CSR-Datei aus.

CSR (PKCS#10) upload

Here you can apply for a new certificate.

Certificate profile **Web Server**

The chosen "Certificate profile" determines the possible usages of the certificate. (Description of certificate profiles [German])

Email addresses with domain names from this list can be used without further confirmation. Email addresses with all other domain names must be confirmed separately.

You can use the following domain names in the CN attribute and SubjectAlternativeNames of type 'DNS':

To upload your own CSR (PKCS#10) file you must have generated it locally, e.g. with openssl.

doku.rz.hs-fulda.de.csr Browse

CSR for doku.rz.hs-fulda.de
Your existing CSR (PKCS#10) file in PEM format. Commonly used file extensions are .pem and .csr.

Your data

Enter further data below. What you enter here will not be found in the certificate.

Full name *
Sven Reissmann ✓

Email *
sven.reissmann@rz.hs-fulda.de ✓

Department
RZ ✓

Revocation PIN *
***** ✓

Revocation PIN - Confirmation *
***** ✓

This PIN is required if you want to revoke your certificate. Please make a note of this PIN.

Personal note

You may enter an optional note for this certificate application here. The comment will solely be saved in your local certificate application data file.

Personal note

I am committed to comply with the regulations contained in [Informationen für Zertifikatinhaber](#). *

I agree to the publication of the certificate with the contained names and e-mail addresses.
You can withdraw this agreement by sending an e-mail to pki@dfn.de. *

I have read the [information about the processing of my personal data for the certificate issuance from DFN-PKI](#). The processing of personal data takes place on the basis of Art. 6 (1) (b) GDPR for the fulfillment of a contract between the DFN Association and the requesting participant institution. The data will be deleted after termination of the contract, as far as there are no obstacles to the deletion of the data. *

Next

Die darauf folgende Seite bietet Ihnen an, den Zertifikatsantrag auszudrucken. Bitte tun Sie dies, unterschreiben Sie den Antrag und bringen Sie diesen zusammen mit einem Ausweisdokument in das Rechenzentrum. Falls Sie im Rechenzentrum bereits bekannt sind bzw. schon zuvor Zertifikate beantragt haben, können Sie den Antrag auch per Hauspost zu uns senden.

Zertifikat erhalten

Nachdem Ihr Antrag geprüft und bestätigt wurde, erhalten Sie das Zertifikat per E-Mail. In Kombination mit dem Ihnen bereits vorliegenden privaten Schlüssel kann das Zertifikat nun auf Ihrem Server verwendet werden.

Da die DFN PKI sog. Intermediate Zertifikate nutzt, müssen diese in der Regel ebenfalls auf Ihrem Server hinterlegt werden. Die aktuelle Zertifikatskette finden sie [hier](#).

From:
<https://doku.rz.hs-fulda.de/> - **Dokumentation des Rechenzentrums**

Permanent link:
<https://doku.rz.hs-fulda.de/doku.php/docs:dfnpki:serverzertifikat>

Last update: **12.04.2022 16:01**

