Beantragung von Serverzertifikaten

*(Hinweis: **eigener** bedeutet in unserem Fall gehört zur Bauhaus-Universität Weimar)*

Fall 1 – eigener Server, eigener Admin, eigene Domain

(Maßgeblich ist der angezeigte Domaininhaber bei einer whois-Abfrage, beispielsweise hier: https://www.denic.de/webwhois/)

Antragsteller: Server-Administrator des eigenen Servers
Antragstellung bei: DFN-PKI Teilnehmerservice der eigenen Einrichtung
Ablauf:

Standardverfahren zur Beantragung von Zertifikaten über eigene DFN-PKI Webschnittstelle

Fall 2 – eigener Server, eigener Admin, fremde Domain *(andere Hochschule)*

Antragsteller: Server-Administrator des eigenen Servers
Antragstellung bei: DFN-PKI Teilnehmerservice der eigenen Einrichtung
Ablauf:

Inhaber der fremden Domain füllt ein so genanntes **Domain-Autorisierungsschreiben** aus, Muster:

Sehr geehrte Damen und Herren,

hiermit gewähren wir der *(Name der eigenen)* Universität das Recht, im Rahmen der DFN-PKI
* beliebige Zertifikate für die folgende Domain zu erhalten:
* *fremde Domain*

---
bzw.:

* beliebige Zertifikate für die folgenden Hostnamen zu erhalten:

    * sharepoint.fremde-domain.de
    * autodiscover.fremde-domain.de
    * group.fremde-domain.de

(Hier die Hostnamen auflisten, die benötigt werden, bzw. diesen Absatz weglassen, wenn die Autorisierung generell für die Domain gelten soll)

<Unterschrift: zeichnungsberechtigter Domaininhaber/Admin-C/Tech-C>

Schreiben vom Domaininhaber an die folgende Adresse schicken:

DFN-CERT Services GmbH
DFN-PCA

Sachsenstraße 5
20097 Hamburg

weiter mit Standardverfahren über eigene DFN-PKI Webschnittstelle

Fall 3 – fremder Server, fremder Admin, eigene Domain

Antragsteller: Server-Administrator des fremden Servers
Antragstellung bei: DFN-PKI Teilnehmerservice der fremden Einrichtung
Ablauf:

Wir (= Inhaber der eigenen Domain) füllen ein so genanntes **Domain-Autorisierungsschreiben** aus, Muster:

Sehr geehrte Damen und Herren,

hiermit gewähren wir der *(Name der fremden Einrichtung, beispielsweise „TU Ilmenau")* das Recht, im Rahmen der DFN-PKI
* beliebige Zertifikate für die folgende Domain zu erhalten:
* *uni-weimar.de*
---
bzw.:

* beliebige Zertifikate für die folgenden Hostnamen zu erhalten:

    ** sharepoint.uni-weimar.de*
    ** autodiscover.uni-weimar.de*
    ** group.uni-weimar.de*
    (= Beispiele)

(Hier die Hostnamen auflisten, die benötigt werden, bzw. diesen Absatz weglassen, wenn die Autorisierung generell für die Domain gelten soll)

<Unterschrift: zeichnungsberechtigter Domaininhaber/Admin-C/Tech-C für unsere Domain uni-weimar.de>

Wir (= Domaininhaber) senden das Schreiben an die folgende Adresse:

DFN-CERT Services GmbH
DFN-PCA
Sachsenstraße 5
20097 Hamburg

weiter mit Standardverfahren über fremde DFN-PKI Webschnittstelle durch fremden Server-Administrator

Fall 4 – eigener Server, fremder Admin, eigene Domain

wie Fall 1

+ Serverbetreuung durch eine Vereinbarung/Vertrag/Kooperation mit eigener Einrichtung geregelt

+ Sollte der Zertifikatantrag durch den Mitarbeiter der anderen Hochschule unterschrieben sein, so ist noch zu prüfen, ob

1. der beantragende Mitarbeiter autorisiert ist, das Zertifikat für die enthaltenen Host-Namen zu bekommen; und

2. das Antragsformular tatsächlich von diesem Mitarbeiter unterschrieben wurde.

Letzteres ist am einfachsten, wenn der Antragsteller das Antragsformular im Beisein unseres (des eigenen) Teilnehmerservices unterschreibt, oder wenn dem eigenen Teilnehmerservice schon eine authentische Unterschriftenprobe des Antragstellers vorliegt.

Alternative:

Beantragung des Zertifikats beim DFN-PKI Teilnehmerservice der fremden Hochschule, sofern diese an der DFN-PKI teilnimmt. Das Zertifikat bekommt dann natürlich das Organisations-Attribut (O-Attribut) der anderen Hochschule verpasst, da es von der anderen CA ausgestellt wird.

Fall 5 – eigener Server, fremder Admin, fremde Domain

wie Fall 2

+ Serverbetreuung durch eine Vereinbarung/Vertrag/Kooperation mit eigener Einrichtung geregelt

+ Sollte der Zertifikatantrag durch den Mitarbeiter der anderen Hochschule unterschrieben sein, so ist noch zu prüfen, ob

1. der beantragende Mitarbeiter autorisiert ist, das Zertifikat für die enthaltenen Host-Namen zu bekommen; und

2. das Antragsformular tatsächlich von diesem Mitarbeiter unterschrieben wurde.

Letzteres ist am einfachsten, wenn der Antragsteller das Antragsformular im Beisein unseres (des eigenen) Teilnehmerservices unterschreibt, oder wenn dem eigenen Teilnehmerservice schon eine authentische Unterschriftenprobe des Antragstellers vorliegt.

Alternative:

Beantragung des Zertifikats beim DFN-PKI Teilnehmerservice der fremden Hochschule, sofern diese an der DFN-PKI teilnimmt. Das Zertifikat bekommt dann natürlich das Organisations-Attribut (O-Attribut) der anderen Hochschule verpasst, da es von der anderen CA ausgestellt wird.