

---

## Nutzerzertifikate

Die Fachhochschule Erfurt stellt für Ihre Beschäftigten und Beamten persönliche digitale Zertifikate aus. Damit können u.a. E-Mails signiert (Schutz gegen Fälschung) und auch verschlüsselt sowie elektronische Dokumente unterschrieben werden. Weitere Anwendungsfälle sind z. B. Autorisierung gegenüber IT-Diensten oder passwortfreies Login.

Ein Zertifikat, hier Nutzerzertifikat, ist eine digitale Identität, die durch eine vertrauenswürdige Instanz beglaubigt worden ist. Es fungiert dabei als elektronischer Ausweis. Ein Nutzerzertifikat besteht aus einem öffentlichen und einem privaten Schlüssel.

Der private Schlüssel gehört ausschließlich dem Eigentümer des Nutzerzertifikates, ist geheim und darf auf keinen Fall an Dritte weitergegeben werden. Der private Schlüssel ist durch ein möglichst komplexes Passwort zu schützen.

Der öffentliche Schlüssel hingegen sollte möglichst allen bekannt sein, da mit Hilfe dieses Schlüssels andere Personen Ihnen z. B. verschlüsselte E-Mails schicken können. Durch die Public-Key-Infrastruktur (PKI) des Deutschen Forschungsnetzwerkes (DFN) wird sichergestellt, dass Ihr öffentlicher Schlüssel auch tatsächlich von Ihnen stammt, indem er signiert wurde.

Digitale Zertifikate werden von einer Certificate Authority (CA) ausgestellt. Die CA bestätigt durch die Ausstellung des digitalen Zertifikats die Identität des Besitzers.

Mit Beendigung des Beschäftigungs-/Beamtenverhältnisses gleich aus welchem Grund (Ende einer Befristung, Aufhebung, Kündigung, Renten- bzw. Pensionseintritt, u. a.) wird das digitale Zertifikat automatisch gesperrt.

## Inhalt

1	Persönliches Nutzerzertifikat beantragen.....	2
2	Nutzerzertifikat im Browser importieren (Mozilla Firefox) .....	6
3	Nutzerzertifikat in GroupWise verwenden (E-Mails signieren) .....	7
4	Nutzerzertifikat in Adobe Acrobat importieren (PDFs unterschreiben) .....	8

# 1 Persönliches Nutzerzertifikat beantragen

1. Verwenden Sie zur Beantragung des persönlichen Nutzerzertifikates den Browser **Mozilla Firefox**.
2. Rufen Sie die Antragsseite auf, um einen Zertifikatsantrag zu erzeugen.

<https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/1440>



3. Wählen Sie „Ein neues Nutzerzertifikat beantragen“.

[Datenschutz](#) | [Impressum](#) | [Zertifizierungsrichtlinie](#)

4. Füllen Sie das Formular aus. Bei Namen tragen Sie bitte Ihren Vor- und Nachnamen **OHNE Umlaute** ein. Weiterhin sind Titel zugelassen, die in Ihrem Personalausweis eingetragen sind, z.B. Dr. Bei **Abteilung** tragen Sie bitte die offizielle Abkürzung für Ihr Institut bzw. die Abteilung ein, z.B. DPR, WGB, BKR, GTI, ISP, IVR, ....

5. Den Namensraum können Sie frei wählen. <sup>1</sup>

<sup>1</sup> Diese Informationen können andere in Ihrem Zertifikat einsehen.

6. Die Sperr-PIN, die mindestens 8-stellig sein muss und aus 8 beliebige Zeichen bestehen kann, dient dazu, Ihr Nutzerzertifikat zu widerrufen, falls dies einmal notwendig sein sollte.<sup>2</sup>
7. Verpflichten Sie sich mit Bestätigung durch das Setzen des Häkchens zur Einhaltung der Regelungen.
8. Stimmen Sie durch das Setzen des Häkchens der Veröffentlichung des Zertifikats zu.<sup>3</sup>
9. Klicken Sie auf „Weiter“.
10. Um das beantragte Zertifikat zu erhalten, befolgen Sie die folgenden Punkte:



## Ihr Zertifikatantrag

Führen Sie jetzt noch folgende Schritte durch:

1. Überprüfen Sie bitte Ihre Angaben auf Richtigkeit. Über den "Daten ändern"-Button können Sie alle Daten ändern.
2. Bitte klicken Sie auf den Button "Antragsdatei speichern". Sie werden aufgefordert ein Passwort für die Antragsdatei und den enthaltenen privaten Schlüssel zu setzen und die Datei auf Ihrem Gerät abzuspeichern. Sie benötigen diese Antragsdatei und das zugehörige Passwort wieder, wenn das beantragte Zertifikat ausgestellt wurde.
3. Laden Sie auf der nächsten Seite das Zertifikatantragsformular (PDF) herunter und geben Sie es vollständig ausgefüllt und unterschrieben an Ihren lokalen DFN-PKI Teilnehmerservice.

11. Überprüfen Sie Ihre Angaben.

### Zertifikatsdaten

E-Mail (emailAddress)	@fh-erfurt.de
Name (CN)	
Organisationseinheit (OU)	HRZ
Organisation (O)	Fachhochschule Erfurt
Standort (L)	Erfurt
Bundesland (ST)	Thüringen
Land (C)	DE

### Zusätzliche Daten

Name	
E-Mail	@fh-erfurt.de
Veröffentlichen	Ihr Zertifikat wird veröffentlicht.
Datum	23.3.2020
Persönliche Notiz	

**Wichtig:** Wenn Sie die Antragsdatei verlieren, bevor die Ausstellung des Zertifikats abgeschlossen ist, gehen auch die Daten unwiederbringlich verloren und der Vorgang muss wiederholt werden.

**Antragsdatei speichern**

Daten ändern

12. Über „Antragsdatei speichern“ speichern Sie Ihren privaten Schlüssel inkl. dem Antrag in einer Datei. Diese benötigen Sie nach der Genehmigung wieder.

<sup>2</sup> Sollten Sie diese PIN vergessen, kann das Zertifikat auch durch das HRZ gesperrt werden. Dazu senden Sie bitte eine Mail an 333@fh-erfurt.de .

<sup>3</sup> Die Veröffentlichung ist notwendig, wenn andere Personen Ihr Zertifikat über die DFN PKI finden sollen.

13. Setzen Sie ein sicheres Passwort für die Antragsdatei.

14. Speichern Sie die Antragsdatei an einem sicheren Ort, z.B. Ihrem Homelaufwerk.

15. Drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn im HRZ vor. Mitzubringen sind das unterschriebene Antragsformular und ein gültiges Ausweisdokument.

Die Sprechzeiten sind immer  
mittwochs  
von 9:00 bis 12:00 Uhr.

Nach der Identitätsprüfung im HRZ erhalten Sie vom DFN eine E-Mail mit einem Link, über den Sie Ihr signiertes Nutzerzertifikat erhalten. Das persönliche Zertifikat in der E-Mail der CA ist nur der öffentliche Schlüssel, elektronisch signiert durch die CA.

Um das Zertifikat verwenden zu können, muss es mit dem privaten Schlüssel zusammengeführt werden. Der private Schlüssel ist in der Antragsdatei enthalten.

16. Öffnen Sie im Mozilla Firefox den Link aus der DFN-Mail unter dem Text

„Wenn Sie ein Nutzerzertifikat beantragt haben, wählen Sie bitte...

17. Wählen Sie „Ein beantragtes Zertifikat abholen“.

Willkommen zu den Antragsseiten der DFN-PKI

Hier können Sie Zertifikate beantragen oder Ihre beantragten und von Ihrem Teilnehmerservice ausgestellten Zertifikate abholen.

Ein neues Nutzerzertifikat beantragen.

Ein beantragtes Zertifikat abholen.

[Datenschutz](#) | [Impressum](#) | [Zertifizierungsrichtlinie](#)

18. Browsen Sie zum Ablageort Ihrer Antragsdatei (z.B. Homelaufwerk).

Geben Sie das Passwort für die Antragsdatei ein, welches Sie in Schritt 13 festgelegt haben und klicken auf „Weiter“.

Zertifikat abholen

Um ein von Ihnen beantragtes Zertifikat abzuholen, benötigen Sie die Antragsdatei, die Sie bei der Antragsstellung gespeichert haben.

Antragsdatei

Antrag vom 23.3.2020 für 11 \* vom 23.3.2020  
Ihre Antragsdatei mit der Dateiendung .json

Bitte geben Sie hier Ihr Passwort ein, mit dem die Antragsdatei geschützt ist.

Das Passwort ist korrekt.

Das Passwort haben Sie bei der Antragsstellung beim Abspeichern der Antragsdatei vergeben.

[Datenschutz](#) | [Impressum](#) | [Zertifizierungsrichtlinie](#)

19. Wählen Sie „Zertifikatsdatei speichern“.

Zertifikat abholen

Folgendes Zertifikat wurde für Sie ausgestellt. Klicken Sie auf den Button "Zertifikatsdatei speichern", um das Zertifikat zusammen mit dem privaten Schlüssel im Format PKCS#12 (Dateiendung .p12) auf Ihrem Gerät abzuspeichern.

Name des Zertifikatinhabers	CN= , OU= , O=Fachhochschule Erfurt, L=Erfurt, ST=Thüringen, C=DE
Teilnehmerservice	FH-Erfurt-CA - G2
Name des Zertifikatsausstellers	CN=DFN-Verein Global Issuing CA, OU=DFN-PKI, O=Verein zur Förderung eines Deutschen Forschungsnetzes e. V., C=DE
Gültig ab	23.3.2020
Gültig bis	23.3.2023
Zertifikatsseriennummer	107064L 1743254474821
Antrag vom	23.3.2020
Persönliche Notiz	
Antragsnummer	51 112

[Datenschutz](#) | [Impressum](#) | [Zertifizierungsrichtlinie](#)

20. Geben Sie ein neues Passwort<sup>4</sup> zum Schutz Ihrer abgespeicherten Zertifikatsdatei ein.

Zertifikatpasswort setzen

Bitte setzen Sie ein Passwort zum Schutz Ihrer Zertifikatsdatei.

Passwort

Passwort bestätigen

Bitte wählen Sie ein neues Passwort (mindestens 8 Zeichen).

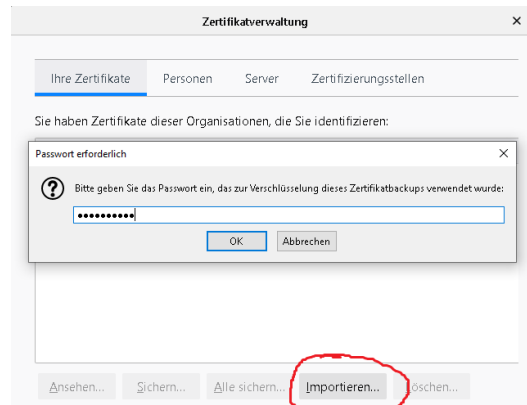
21. Speichern Sie Ihr Nutzerzertifikat (\*.p12 Datei) auf Ihrem Homelaufwerk.

Die Datei enthält den privaten UND öffentlichen Schlüssel und kann in andere Anwendungen, z.B. Browser und Mail-Clients importiert werden.

<sup>4</sup> Dieses Passwort schützt Ihr persönliches Zertifikat vor missbräuchlicher Verwendung durch Dritte. Es sollte daher besonders sicher sein. Sie benötigen dieses Passwort, wenn Sie ihr Zertifikat in eine Anwendung importieren und dort verwenden wollen.

## 2 Nutzerzertifikat im Browser importieren (Mozilla Firefox)

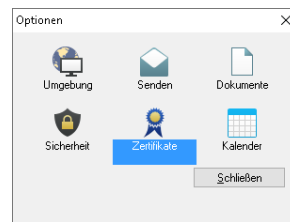
1. Importieren Sie Ihr Zertifikat in den Browser  
Öffnen Sie die Einstellungen unter Datenschutz und Sicherheit. Wählen Sie „Zertifikate anzeigen“.
2. Wählen Sie die Reiterkarte „Ihre Zertifikate“, wählen „Importieren“ und suchen die gespeicherte Zertifikatsdatei (\*.p12). Bestätigen Sie den Import mit dem von Ihnen beim Speichern festgelegten Passwort aus Schritt **Fehler! Verweisquelle konnte nicht gefunden werden..**



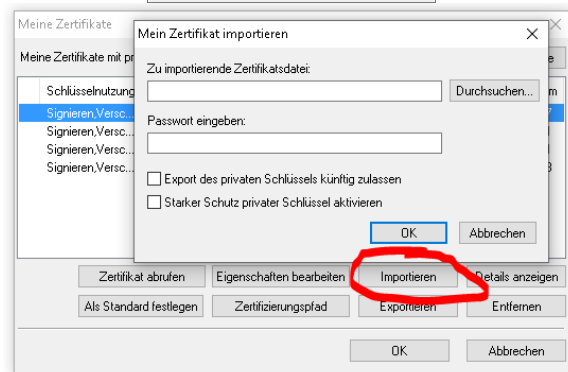
Nun befindet sich das persönliche Zertifikat (privater UND öffentlicher Schlüssel) im Zertifikatspeicher des Browsers.

### 3 Nutzerzertifikat in GroupWise verwenden (E-Mails signieren)

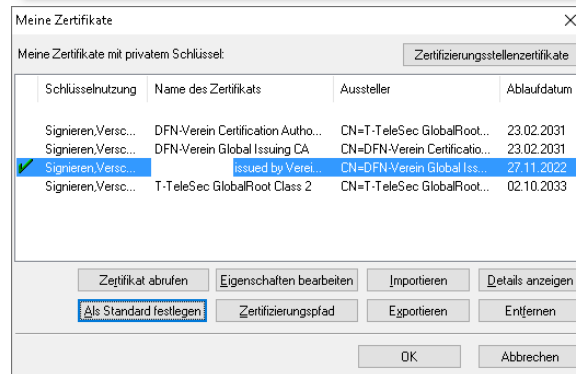
1. Unter GroupWise „Optionen“  
„Zertifikate“ aufrufen.



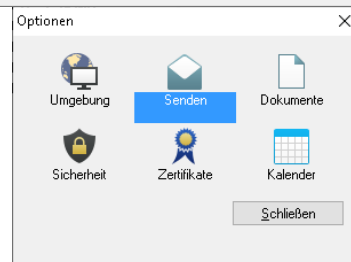
2. Über den Button „Importieren“ die  
Zertifikatsdatei (\*.p12) auswählen  
und das gesetzte Passwort  
eingeben.  
Das Häkchen bei „Export des  
privaten Schlüssel aktivieren“  
entfernen<sup>5</sup>.



3. Das Nutzerzertifikat auswählen  
und „Als Standard festlegen“.

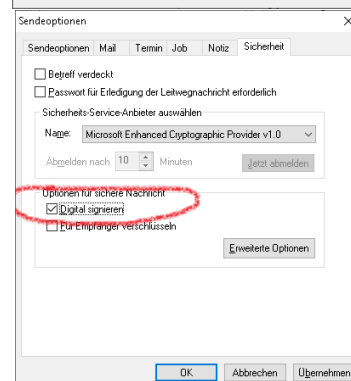


4. Unter GroupWise  
„Optionen“,  
„Senden“



„Senden“  
aufrufen.

5. Unter der Reiterkarte „Sicherheit“  
im Feld Optionen für sichere  
Nachricht das Häkchen bei  
„Digital signieren“ setzen.

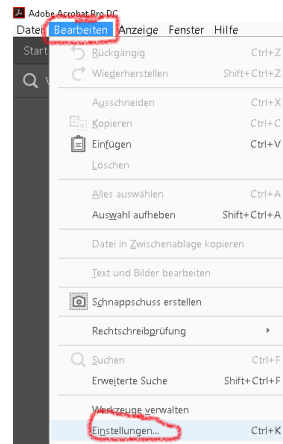


Ab jetzt wird jede ausgehende Nachricht mit dem Nutzerzertifikat digital signiert.

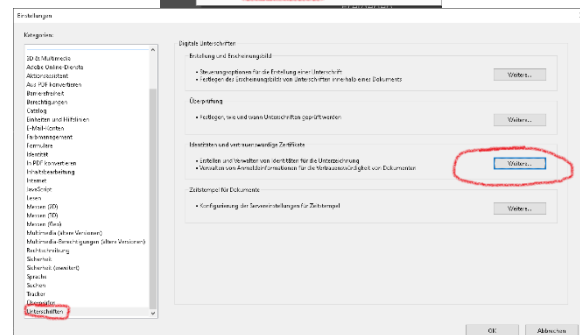
<sup>5</sup> Da Sie Ihr Zertifikat bereits im \*.p12-Format haben, können Sie diese Option deaktivieren.

## 4 Nutzerzertifikat in Adobe Acrobat importieren (PDFs unterschreiben)

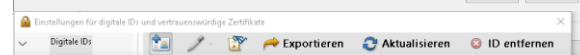
1. Öffnen Sie im Adobe Acrobat DC unter „Bearbeiten“ den Menüpunkt „Einstellungen“.



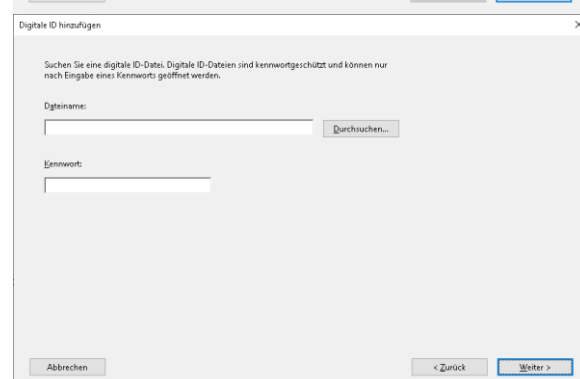
2. Wählen Sie den Menüpunkt „Unterschriften“ und klicken im Bereich „Identitäten und vertrauenswürdige Zertifikate“ den Button „Weitere“



3. Wenn Ihr Nutzerzertifikat noch nicht aufgelistet ist, dann importieren Sie es über das Icon mit der „Kontaktkarte“, wählen „Datei“,

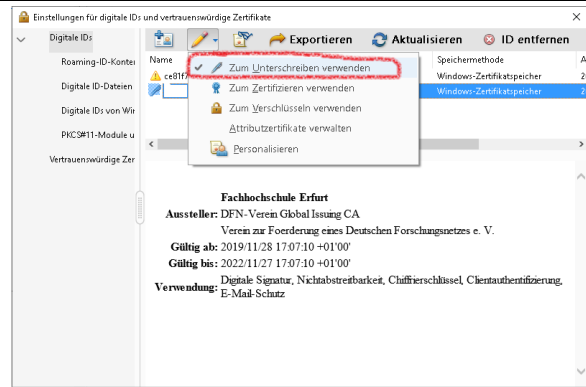


4. und suchen Ihre Zertifikatsdatei (\*.p12) und geben Ihr Passwort ein.

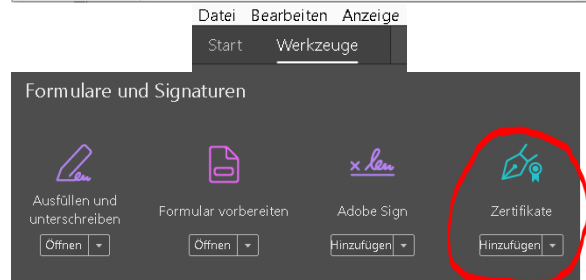




5. Wählen Sie nun Ihr Nutzerzertifikat aus und legen Sie die jeweilige Verwendung mit Hilfe des „Stifts“ fest: z. B. „Zum Unterschreiben verwenden“. Das Fenster kann im Anschluss geschlossen werden.



6. Zum Unterschreiben öffnen Sie das entsprechende Dokument, wählen unter Werkzeuge im Bereich „Formulare und Signaturen“ den Punkt „Zertifikate“.



7. Im Dokument wählen Sie aus der Werkzeugleiste „Digital unterschreiben“ und Ihr Nutzerzertifikat aus.

