

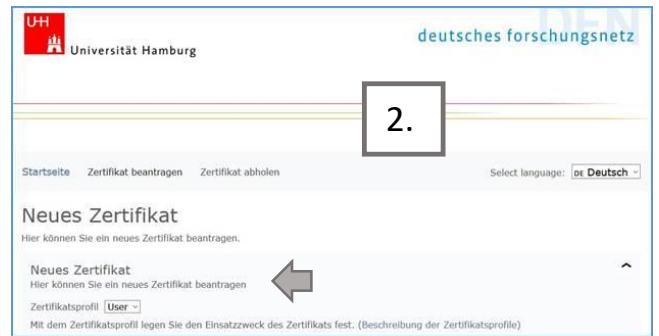
# Persönliches Zertifikat beantragen und in Outlook einbinden

Die digitale ID ermöglicht die Überprüfung der Authentizität des Senders und trägt damit dazu bei, die Manipulation von Nachrichten zu verhindern. Die digitale Signatur erhöht also die Sicherheit beim Versand und Empfang von eMail-Nachrichten.

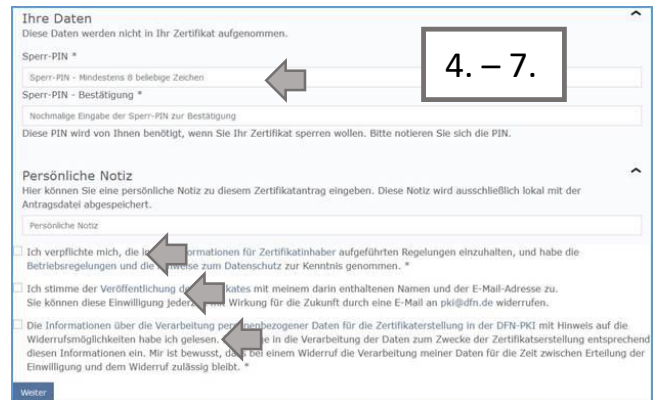
Voraussetzung: eine gültige B-Kennung + Passwort + ein gültiger deutscher Personalausweis

Stellen Sie den Antrag von ihrem Arbeitsplatzrechner aus, nicht von einem „fremden“ Rechner oder einem anderen Mobilgerät.

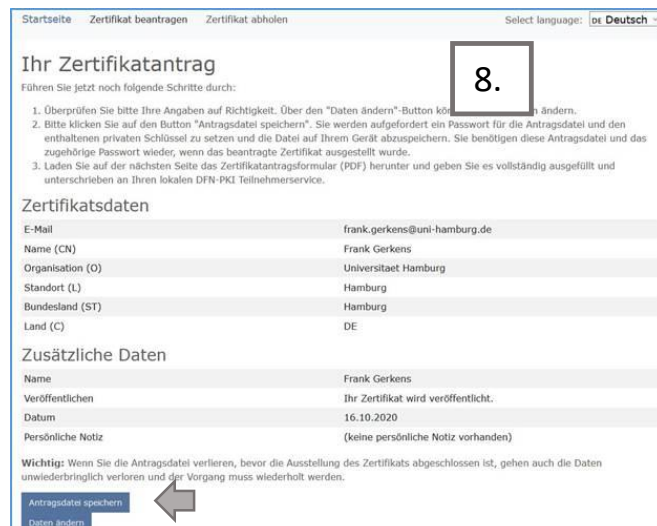
1. Beantragen Sie hier das Nutzerzertifikat: <https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/4430>
2. Gehen Sie auf „Ein neues Nutzerzertifikat beantragen“



3. Geben Sie ein: Ihren Namen, Ihre eMail-Adresse, Ihre Abteilung (freiwillig), Namensraum (freiwillig)
4. Unter „Ihre Daten“ wählen Sie eine mind. 8stellige PIN
5. Setzen Sie die Haken bei: Ich verpflichte mich...
6. Ich stimme der Veröffentlichung des Zertifikats zu...
7. Ich habe gelesen...und weiter



8. Speichern Sie die Antragsdatei
9. Setzen Sie ein Passwort für die Antragsdatei (nicht das gleiche Passwort, wie für die PIN)



- Laden Sie die Datei auf Ihren Rechner und öffnen Sie sie anschließend
- Drucken Sie das Antragsformular aus und unterzeichnen Sie es

10.

Zertifikat beantragen

Ihr Zertifikatantrag

Laden Sie das Zertifikatantragsformular (PDF) herunter und geben Sie es vollständig ausgefüllt und unterschrieben an Ihren lokalen DFN-PKI Teildienstleister.

Zertifikatantragsformular (PDF) herunterladen

11.

Zertifikatantrag für ein Nutzerzertifikat

Antragsnummer

Antragsteller

Vorname Nachname: Frank Gerkens

E-Mail: frank.gerkens@uni-hamburg.de

Abteilung

Zertifikatsdaten

Eindeutiger Name

Alternativer Name: email:frank.gerkens@uni-hamburg.de

Public Key Fingerprint

Veröffentlichen: Ja

Zertifikatprofil: User

Erklärung des Antragstellers

Hiemit beantrage ich ein Nutzerzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter [https://info.pca.dfn.de/doc/info\\_Zertifikatanhaber.pdf](https://info.pca.dfn.de/doc/info_Zertifikatanhaber.pdf) veröffentlichten „Informationen für Zertifikatanhaber“ einzuhalten. Das heißt insbesondere:

- Ich darf den privaten Schlüssel zu dem Zertifikat nicht anderen Personen zugänglich machen. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem ich den privaten Schlüssel speichere bzw. einsetze, muss angemessen geschützt, also z. B. frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
- Ich bin unter den folgenden Bedingungen verpflichtet, das Zertifikat sperren zu lassen:
  - Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
  - Der private Schlüssel oder die dazugehörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
  - Ich bin nicht mehr berechtigt, das Zertifikat zu nutzen.

Die beiliegende bzw. bei web-basierter Antragstellung unter <https://info.pca.dfn.de/doc/datenschutz.html> abrufbaren Informationen über die Verarbeitung personenbezogener Daten für die Zertifikatserteilung in der DFN-PKI mit Hinweis auf die Widerrufsmöglichkeiten habe ich gelesen. Ich willige in die Verarbeitung der Daten zum Zwecke der Zertifikatserteilung entsprechend diesen Informationen ein. Mir ist bewusst, dass bei einem Widerruf die Verarbeitung meiner Daten für die Zeit zwischen Erteilung der Einwilligung und dem Widerruf zulässig bleibt.

(Ort, Datum) (Unterschrift)

Wird vom Teildienstleister ausgefüllt

Identitätsprüfung:

- Name geprüft
- Unterschrift geprüft
- Bild geprüft
- Ausweisgültigkeit geprüft
- Amtliches Ausweispapier mit Lichtbild:

Antragsprüfung:

- Berechtigung des Antragstellers zum Erhalt des beantragten Zertifikats geprüft
- E-Mail-Adresse(n) sind dem Antragsteller zugeordnet
- Eindeutiger Name (s.o.) noch nicht an andere Person vergeben

Name des TS-Mitarbeiters: \_\_\_\_\_

Zugehörige TS-Stelle: \_\_\_\_\_

(Datum, Unterschrift)

Seite 1/1 (Antragsnummer 67 732 256) dfn-ca-globa1-g2, RA-ID: 4430

12.

Regionales Rechenzentrum der Universität Hamburg

Schlüterstr. 70  
20146 Hamburg

Mitarbeiter Name, Vorname	Durchwahl	Raumnummer	E-Mail
	040-42838-	Schlüterstr. 70	uhh-ra@uni-hamburg.de oder...
Baftijari, Jasir	4625	417 S	jasir.baftijari@uni-hamburg.de
Kurtz, Reinhardt	7977	419a S	reinhardt.kurtz@uni-hamburg.de

- Vereinbaren Sie einen Termin mit einem RRZ-Mitarbeiter [jasir.baftijari@uni-hamburg.de](mailto:jasir.baftijari@uni-hamburg.de) oder [reinhard.kurtz@uni-hamburg.de](mailto:reinhard.kurtz@uni-hamburg.de)

**Authentifizierung:** Sie werden aufgefordert, das unterzeichnete Zertifikat per eMail an den Mitarbeiter zu senden. Sie erhalten einen Zoom-Terminvorschlag. Halten Sie den Zertifikatantrag und ihren Personalausweis zu diesem Termin griffbereit.

- Wurde ihr Antrag bearbeitet, können Sie ihr Zertifikat auf der Startseite (Zertifikat abholen) abholen

13.

Zertifikat abholen

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

Antragsdatei\_Fränk\_Gerkens\_67732256\_2020-10-16.json

Antrag 67732256 für "Fränk Gerkens" vom 16.10.2020

Ihre Antragsdatei mit der Dateiendung .json:

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

.....

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

Haben Sie das Zertifikat erhalten, können Sie es mit der empfohlenen Anleitung <https://www.rrz.uni-hamburg.de/services/e-mail/fuer-mitarbeiter/exchange/handouts/handout-einbindung-eines-persoelichen-zertifikats-in-outlook.pdf> in Outlook einbinden.