

# Beantragung eines persönlichen Zertifikats

---

## 1. Informationsübersicht

Mithilfe der personenbezogenen Zertifikate kann sichergestellt werden, dass eine mit dem Zertifikat digital unterschriebene E-Mail eindeutig von der angegebenen Person stammt. Die von der UHH ausgestellten persönlichen Zertifikate werden also u.a. zum Signieren und Verschlüsseln von E-Mails benutzt.

An dieser Stelle wird eine kurze Darstellung der nötigen Schritte zur Beantragung eines persönlichen Zertifikats dargestellt. Dies ersetzt NICHT das ausführliche Lesen der Regeln und Bedingungen zur Nutzung der Zertifikate, sondern dient der Bereitstellung eines übersichtlichen Weges zur Beantragung und Einbindung eines Zertifikats.

Gut zu wissen/vor der Anwendung:

- [2019 liefen eine Reihe alter Zertifikate ab](#) und [es fand eine Umstellung](#) auf die „Global G2 Hierarchie des DFN-Vereins“ statt. Daher sind einzelne Anleitungen des RRZ, [die hier zu finden sind](#), teilweise veraltet.
- [Hier ist ein Überblick](#) über die neuen Zertifikate zu finden, anders als bei den abgelaufenen Zertifikaten funktionieren die neuen „global“, sodass nach der Installation eine manuelle Integration [in einigen gängigen Programmen](#) nicht nötig ist.
- [An dieser Stelle](#) bietet das RRZ Handouts zum Thema E-Mail Zertifikate an.

## 2. Zum persönlichen Zertifikat

Das Rechenzentrum bietet [wichtige Informationen über die Zertifikate an](#). Darüber hinaus sind [an dieser Stelle](#) relevante Informationen über persönliche Zertifikate nachzulesen. Hier sind die Informationen des RRZ [zum Beantragen von persönlichen Zertifikaten](#) zu finden.

Die folgenden Schritte sind nötig, um ein persönliches Zertifikat zu beantragen:

- [Hier](#) können Sie ein Nutzerzertifikat beantragen.
  - Sie klicken auf den Button „Nutzerzertifikat beantragen“ und füllen alle benötigten Informationen aus.
    - Im Rahmen der Beantragung benötigen Sie eine Sperr-PIN mit mind. 8 Zeichen, bitte notieren Sie sich die PIN.
    - Achtung: Es dürfen nur Zertifikate für E-Mail-Adressen mit @uni-hamburg.de ausgestellt werden.
    - Zudem können in der Antragsstellung keine Umlaute verwendet werden, bitte verwenden Sie daher nur Buchstaben ohne Umlaute.
    - Tipp: Schreiben Sie Ihre E-Mail-Adresse immer in Kleinbuchstaben. Dies beugt einigen technischen Fehlern vor.
  - Wenn Sie auf „Weiter“ klicken, erhalten Sie eine Übersicht der eingegebenen Informationen zum Abgleich und können die Antragsdatei **nach dem Festlegen eines Passworts** durch einen Klick auf „Antragsdatei speichern“ herunterladen (es handelt sich um eine Datei mit der Dateiendung \*.json).



[Startseite](#) [Zertifikat beantragen](#) [Zertifikat abholen](#) [Zertifikat sperren](#)

Select language:  
 Deutsch

## 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.

### Zertifikatsdaten

E-Mail	max.mustermann@uni-hamburg.de
Name (CN)	Max Mustermann
Vorname (GN)	Max
Nachname (SN)	Mustermann
Organisation (O)	Universitaet Hamburg
Standort (L)	Hamburg
Bundesland (ST)	Hamburg
Land (C)	DE

### Zusätzliche Daten

Name	Max Mustermann
Veröffentlichen	Ihr Zertifikat wird veröffentlicht.
Datum	18.8.2021
Persönliche Notiz	Nur ein Test zu Anleitungszwecken

**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](#)

- Im nächsten Schritt wird Ihr Zertifikatantrag dargestellt. Sie können bei Bedarf Ihre Antragsdatei erneut speichern und an dieser Stelle auch das im nachfolgenden Schritt benötigte Zertifikatantragsformular als PDF herunterladen.
- Dieses sollten Sie ausdrucken, ausfüllen (bzw. unterschreiben) und schließlich wieder einscannen. Sie benötigen das Antragsformular im nächsten Schritt.

Optional: Es ist möglich, das erhaltene Antragsformular auch mit einer digitalen Unterschrift zu versehen, sodass Sie den Prozess des Ausdruckens, Ausfüllens & Einscannens umgehen könnten. Allerdings ist eine digitale Unterschrift zu diesem Zeitpunkt der Antragstellung noch

unzertifiziert. Wir können also nicht garantieren, dass dies in jedem Fall vom RRZ akzeptiert wird.

Startseite    Zertifikat beantragen \*    Zertifikat abholen    Zertifikat sperren    Select language:   
  Deutsch ▾

## Ihr Zertifikatantrag

Ihr Zertifikatantrag wurde unter der Nummer 123456789 hochgeladen.

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

[Zertifikatantragsformular \(PDF\) herunterladen](#)

Bitte überprüfen Sie, dass das Herunterladen und Speichern der Antragsdatei Antragsdatei\_Test\_2021-07-30.json erfolgreich war. Sollte beim Speichern ein Fehler aufgetreten sein, können Sie die Antragsdatei erneut herunterladen und speichern.

[Antragsdatei \(JSON\) erneut speichern](#)

Sobald Ihr Zertifikat ausgestellt wurde, erhalten Sie eine Benachrichtigung mit allen weiteren nötigen Schritten, um das Zertifikat herunterzuladen und dieses mit dem privaten Schlüssel aus Ihrer Antragsdatei zu einer Zertifikatdatei (.p12) zu verbinden.

- Als Mitglied der Fakultät für Erziehungswissenschaft müssen Sie das Antragsformular [an das RRZ übermitteln](#). Andere Personen finden [hier](#) die zuständige Teilnehmerservicestelle.
- Dort landen Sie (nach einem etwaigen UHH-Login mit Ihrer UHH-Kennung) beim „Uploadformular PKI-Zertifikatsantrag (RRZ)“.

### UPLOADFORMULAR PKI-ZERTIFIKATSANTRAG (RRZ)

Felder mit einem \* sind Pflichtfelder und müssen ausgefüllt werden.

**Beantragende Person**

Name:

B-Kennung:

E-Mail-Adresse:

Durchwahl:

**Antragsformular als Anhang (zwingend erforderlich)**

Anhang:  keine Dateien ausgewählt.

- Lesen Sie sich die darunter liegende Erklärung gründlich durch, füllen Sie die benötigten Eingaben aus, laden Sie ihr unterschriebenes Antragsformular hoch und bestätigen Sie anschließend Ihre Zustimmung durch das Ankreuzen der Kästchen und einen Klick auf „Weiter“.
- Es wird automatisch ein RRZ Support-Ticket eröffnet und Sie erhalten eine automatisch generierte E-Mail.
- Sobald Ihr Ticket bearbeitet wird, erhalten Sie eine Antwort des RRZ mit Terminvorschlägen für eine Identitätsprüfung via Zoom-Videokonferenz.
  - Sollten zu diesem Zeitpunkt Fehler in Ihrem Antrag sein, erhalten Sie statt des Terminvorschlags eine Nachricht des RRZ, dass Ihr Antrag nicht weiterbearbeitet werden konnte. In dem Fall müssen Sie einen neuen Antrag stellen.
- Für den Zoom-Termin zur Identitätsprüfung benötigen Sie
  - Ihren Zertifikatsantrag (bzw. die Antragsnummer),
  - einen gültigen deutschen Personalausweis,



- eine Webcam mit ausreichend guter Videoqualität, um die Sicherheitsmerkmale des Ausweises erkennen zu können.
- Nach der erfolgreichen Identitätsprüfung erhalten Sie eine E-Mail mit weiteren Informationen und Ihrem eigenen Zertifikat (im Format \*.pem) als Dateianhang.  
Zudem ist [ein Link](#) enthalten, über den Sie die Zertifikatdatei im PKCS#12-Format (\*.p12) erstellen können. Diese Datei benötigen Sie, um sie in anderen Programmen (wie Ihrem E-Mail-Programm) einzubinden.  
Für die Erstellung der Zertifikatdatei im PKCS#12-Format benötigen Sie:
  - Ihre ursprünglich heruntergeladene Antragsdatei im \*.json-Format,
  - das von Ihnen im Rahmen des Antrags erstellte Passwort.
  - Zudem werden Sie darum gebeten, für das Zertifikat ein weiteres Passwort zu vergeben.
- Die erstellte Zertifikatdatei können Sie nun in den benötigten Programmen importieren.

### 3. Nutzung

Mit dem Zertifikat können Sie [PDFs digital unterschreiben](#) und [E-Mails z.B. mit Thunderbird signieren und verschlüsseln](#). Alternativ können Sie hierfür auch [Outlook](#) nutzen.