

SHORTGUIDE BEANTRAGUNG EINES PERSÖNLICHEN NUTZER- ZERTIFIKATS

FÜR MITGLIEDER UND ANGEHÖRIGE DER RUB

Persönliche Nutzerzertifikate

Das digitale Zertifikat ist ein Datensatz, der die Identität des Inhabers bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Zertifikate sind Grundlagen für digitale Signaturen und Verschlüsselung und bilden somit die Grundlage sicherer Kommunikation im Netz.

Die Nutzerzertifikate stehen allen Mitgliedern und Angehörigen der RUB zur Verfügung. Persönliche Nutzerzertifikate eignen sich für das Signieren (z.B. von E-Mails) sowie zur Verschlüsselung und Authentifizierung.

Wie entsteht mein Nutzerzertifikat?

Sie beantragen Ihr Nutzerzertifikat in Ihrem Browser. Der Browser erzeugt dabei ein Schlüsselpaar: Der geheime (private) Teil des Schlüssels verbleibt im Browser, der öffentliche Teil des Schlüssels wird dem DFN-Verein übermittelt. IT.SERVICES gibt Ihren Antrag nach Identitätsprüfung frei. Der DFN-Verein benachrichtigt Sie per E-Mail, sobald das Zertifikat beglaubigt ist. Erst durch die Zusammenführung des geheimen Schlüssels und des durch den DFN beglaubigten Teils in Ihrem Browser entsteht das Zertifikat. Dieses kann exportiert werden, um sicher abgelegt und in anderen Programmen verwendet werden zu können.

Die nachfolgende Anleitung beschreibt Ihnen Schritt für Schritt, wie Ihr persönliches Nutzerzertifikat beantragt, ausgestellt und gesichert wird.

Beantragung eines persönlichen Nutzerzertifikats

Die Beantragung erfolgt über das DFN-PKI-Portal:

<https://pki.pca.dfn.de/uni-bochum-ca-g2/pub>

Bei Fragen können Sie Kontakt mit der Registrierungsstelle aufnehmen: pki@ruhr-uni-bochum.de oder telefonisch im Servicecenter unter 0234/32-24025.

Hinweis:

Für Gruppenzertifikate stellen Sie das Kürzel „GRP:“ voran

Infoseite zum Zertifikat:

<https://it-services.ruhr-uni-bochum.de/services/ias/antrag-nutzerzertifikat.html.de>

Schritt 1

Lesen Sie sich die Informationen Ausstellung eines persönlichen Nutzerzertifikats durch.

Unter „Ein neues Nutzerzertifikat beantragen“, finden Sie den Link zur Antragsseite.

deutsches

Willkommen zu den Antragsseiten der DFN-PKI

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

Ein neues Nutzerzertifikat beantragen.

Ein beantragtes Zertifikat abholen.

Datenschutz | Impressum | Zertifizierungsrichtlinie

Schritt 2

Füllen Sie den Antrag mit Ihren persönlichen Daten aus, beachten Sie dabei das im Namen keine Um- laute verwendet werden dürfen.

Zertifikatsdaten

Hier können Sie ein neues Zertifikat beantragen

Zertifikatsprofil **User**

Mit dem Zertifikatsprofil legen Sie den Einsatzzweck des Zertifikats fest. (Beschreibung der Zertifikatsprofile)

Neuer Antrag

Antrag erstellen

Aus den folgenden Daten wird ein neuer Zertifikatsantrag generiert.

- E-Mail-Adressen mit folgenden Domainnamen können ohne weitere Bestätigung verwendet werden. E-Mail-Adressen mit anderen Domainnamen müssen separat bestätigt werden.

Name (CN)

E-Mail

Abteilung (OU, optional)

Namensraum (Der endgültige Zertifikatsname wird mit dem gewählten Namensraum vervollständigt.)
 O=Ruhr-Universitaet Bochum,C=DE

Ihre Daten

Diese Daten werden nicht in Ihr Zertifikat aufgenommen.

Sperr-PIN

Sperr-PIN - Bestätigung

Diese PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen. Bitte notieren Sie sich die PIN.

Persönliche Notiz (Optional)

Hier können Sie eine persönliche Notiz zu diesem Zertifikatsantrag eingeben. Diese Notiz wird ausschließlich lokal mit der Antragsdatei abgespeichert.

Persönliche Notiz (Optional)

- Ich verpflichte mich, die in den Informationen für Zertifikathaber aufgeführten Regelungen einzuhalten.
- Optional: Ich stimme der Veröffentlichung des Zertifikates mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu. Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an pki@dfn.de widerrufen.

[Weiter](#)

Schritt 3

Jetzt haben Sie nochmal die Möglichkeit alle auf Richtigkeit zu prüfen und gegebenenfalls zu korrigieren.

Antragsdatei speichern, merken Sie sich, wohin die Datei gespeichert wird. Sie benötigen sie später nochmals. In der Regel wird die Datei im Download Ordner gespeichert.

Merken Sie sich das Passwort, das Sie setzen gut. Sie benötigen es, um das Zertifikat zu erhalten.

Nun den Zertifikatsantrag heruntergeladen, ausdrucken und unterschreiben. Das Zertifikat muss unter Vorlage des Personal- ausweis **persönlich** im Servicecenter von IT:Services (IA E0 150/95) abgegeben werden. Nicht alle MitarbeiterInnen des Servicecenter dürfen Zertifikate genehmigen, darum ist eine telefonisch (Tel.: 24025) Voranmeldung sinnvoll.

Ihr Zertifikatsantrag

Führen Sie jetzt noch folgende Schritte durch:

- Überprüfen Sie bitte Ihre Angaben auf Richtigkeit. Über den "Daten ändern"-Button können Sie alle Daten ändern.
- 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.
- Laden Sie auf der nächsten Seite das Zertifikatsantragsformular (PDF) herunter und geben Sie es vollständig ausgefüllt und unterschrieben an Ihren lokalen DFN-PKI Teilnehmerseite.

Zertifikatsdaten	
E-Mail (emailAddress)	andreas.mueller@ruhr-uni-bochum.de
Name (CN)	Andreas Müller
Organisationseinheit (OU)	IT-Servicecenter E0 150/95
Organisation (O)	Ruhr-Universitaet Bochum
Land (C)	DE

Zusätzliche Daten	
Name	Andreas Müller
E-Mail	andreas.mueller@ruhr-uni-bochum.de
Veröffentlichen	Ihr Zertifikat wird veröffentlicht.
Datum	8.4.2020
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](#)

Ihr Zertifikatsantrag

Ihr Zertifikatsantrag wurde unter der Nummer ********* hochgeladen.

Laden Sie das Zertifikatsantragsformular (PDF) herunter und geben Sie es vollständig ausgefüllt und unterschrieben an I

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

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

Datenschutz | Impressum | Zertifizierungsrichtlinie

DFN-PKI

Zertifikatsantrag für ein Nutzerzertifikat

an DFN-CA Global Q2

Antragsteller: andreas.mueller@ruhr-uni-bochum.de

Name: Andreas Müller

Abteilung: IT-Servicecenter E0 150/95

Zertifikatsart: Benutzerzertifikat (Schnellzugriff)

Erweiterter Name: andreas.mueller@ruhr-uni-bochum.de

Abteilungskürzel: IT-Servicecenter E0 150/95

Public Key Algorithmus: RSA

Signature Algorithmus: SHA256

Erklärung des Antragszettels

Hier ist ein Antrag zur Erzeugung eines DFN-PKI Zertifikats im Rahmen des DFN-CA Global Q2 Projekts. Das Zertifikat wird ausschließlich für den persönlichen Gebrauch des Antragstellers erstellt.

- Ein Antragsteller muss einen gültigen Personalausweis vorlegen, der bei der Antragstellung noch nicht abgelaufen ist.
- Ein Antragsteller muss einen gültigen E-Mail-Adresse angeben, die mit der DFN-CA Global Q2 kompatibel ist.
- Ein Antragsteller muss einen gültigen Namen angeben, der mit der DFN-CA Global Q2 kompatibel ist.
- Ein Antragsteller muss einen gültigen Abteilungskürzel angeben, der mit der DFN-CA Global Q2 kompatibel ist.
- Ein Antragsteller muss einen gültigen Public Key Algorithmus angeben, der mit der DFN-CA Global Q2 kompatibel ist.
- Ein Antragsteller muss einen gültigen Signature Algorithmus angeben, der mit der DFN-CA Global Q2 kompatibel ist.

Die fertiggestellten, mit dem DFN-PKI Zertifikat verbundenen Daten sind im Download Ordner gespeichert. Sie sind im DFN-PKI Zertifikatsantragsformular (PDF) heruntergeladen und können dort abgerufen werden. Sie sind im DFN-PKI Zertifikatsantragsformular (PDF) heruntergeladen und können dort abgerufen werden. Sie sind im DFN-PKI Zertifikatsantragsformular (PDF) heruntergeladen und können dort abgerufen werden.



Bitte drucken Sie das Zertifikatsantragsformular (PDF) aus und unterschreiben Sie es.


Bitte laden Sie das Zertifikatsantragsformular (PDF) auf Ihrer lokalen DFN-PKI Teilnehmerseite hoch.

Nach der Genehmigung des Zertifikatsantrags erhalten Sie ein Mail vom DFN Verein.


Klicken Sie auf den Link zum Nutzerzertifikat.

RUB CA Zertifikatinformation

 dfnpki-mailsender-noreply@dfn-cert.de
An 
Cc rubca@ruhr-uni-bochum.de
Signiert von dfnpki-mailsender-noreply@dfn-cert.de

 cert-10731-10496410495536960410496035.pem
.pem-Datei

Sehr geehrte Nutzerin, sehr geehrter Nutzer,
die Bearbeitung Ihres Zertifizierungsantrags  mit Profil User ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer  ist auf den Namen CN=, OU=, O=Ruhr-Universitaet Bochum,C=DE erstellt worden.

Sie benötigen die Seriennummer, um Ihr Zertifikat gegebenenfalls sperren zu können.

* Wenn Sie ein Nutzerzertifikat beantragt haben, wählen Sie bitte die folgende Seite. Dort können Sie eine Zertifikatdatei im PK für Ihre Anwendungen benötigen:

<https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/4050/certificates/> 

* Andernfalls, wenn Sie das Zertifikat über den Karteireiter "Serverzertifikat" beantragt haben, benötigen Sie
- die CA-Zertifikate unter der Seite

https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2;RA_ID=4050

Wählen Sie die beim Erzeugen des Antrags gespeicherte Datei aus und geben Sie das Passwort ein, dass Sie bei der Erstellung gewählt haben.

Zertifikat abholen

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

Antragsdatei _2020-04-08.json

Antrag 55585312 für "Anke Woller" vom 8.4.2020
Ihre Antragsdatei mit der Dateieendung .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.



Datenschutz | Impressum | Zertifizierungsrichtlinie

Nun können Sie die Zertifikatsdatei abholen. Speichern Sie die Datei auf Ihrem Rechner so, dass Sie diese wiederfinden.

Zertifikat abholen

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

Name des Zertifikatinhabers	CN=Anke Woller, OU=IT SERVICES SD, O=Ruhr-Universitaet Bochum, C=DE
Teilnehmerservice	RUB CA - G2
Name des Zertifikatsausstellers	CN=DFN-Verein Global Issuing CA, OU=DFN-PKI, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., C=DE
Gültig ab	8.4.2020
Gültig bis	8.4.2023
Zertifikatsseriennummer	
Antrag vom	8.4.2020
Persönliche Notiz	
Antragsnummer	55585312




Wählen Sie ein Passwort und merken Sie sich es!

Zertifikatpasswort setzen

Bitte setzen Sie ein Passwort zum Schutz Ihrer Zertifikatdatei.

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



Ihr Zertifikat ist zusammen mit dessen privaten Schlüssel im Standard-Download-Verzeichnis Ihres Browser oder in dem von Ihnen beim Abspeichern ausgewählten Verzeichnis gespeichert worden. Die Zertifikatdatei liegt im Format PKCS#12 (Dateiendung .p12) vor.

Die Zertifikatdatei ist mit dem von Ihnen vergebenen Passwort geschützt.

Sie können die Zertifikatdatei zur weiteren Verwendung nun in die Software (z.B. Browser, Mail-Programm, Betriebssystem usw.) importieren, in der Sie das Zertifikat nutzen möchten. Sie können die Zertifikatdatei auch auf andere Geräte kopieren, auf denen Sie das Zertifikat nutzen wollen.

Zertifikat abholen

Ihr Zertifikat ist zusammen mit dessen privaten Schlüssel im Standard-Download-Verzeichnis Ihres Browser oder in dem von Ihnen beim Abspeichern ausgewählten Verzeichnis gespeichert worden. Die Zertifikatdatei liegt im Format PKCS#12 (Dateiendung .p12) vor.

Die Zertifikatdatei ist mit dem von Ihnen vergebenen Passwort geschützt.

Sie können die Zertifikatdatei zur weiteren Verwendung nun in die Software (z.B. Browser, Mail-Programm, Betriebssystem usw.) importieren, in der Sie das Zertifikat nutzen möchten. Sie können die Zertifikatdatei auch auf andere Geräte kopieren, auf denen Sie das Zertifikat nutzen wollen.

Backup: Bitte sichern Sie diese Zertifikatdatei und das zugehörige Passwort, so dass beide auch bei Verlust oder Beschädigung Ihres Gerätes noch zur Verfügung stehen, um gegebenenfalls damit verschlüsselte Daten (z.B. E-Mails und Dateien) wieder entschlüsseln zu können.

[Zurück](#)



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

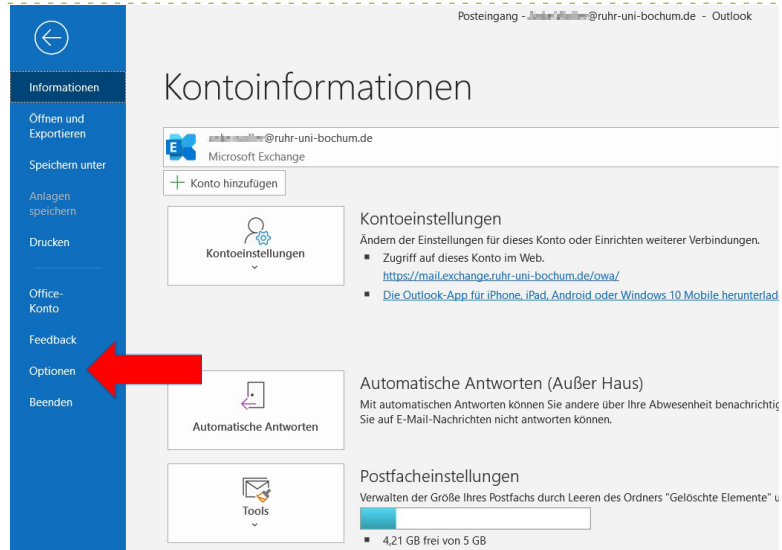
Hinweis

Backup: Bitte sichern Sie diese Zertifikatdatei und das zugehörige Passwort, so dass beide auch bei Verlust oder Beschädigung Ihres Gerätes noch zur Verfügung stehen, um gegebenenfalls damit verschlüsselte Daten (z.B. E-Mails und Dateien) wieder entschlüsseln zu können.

Einbinden in Outlook

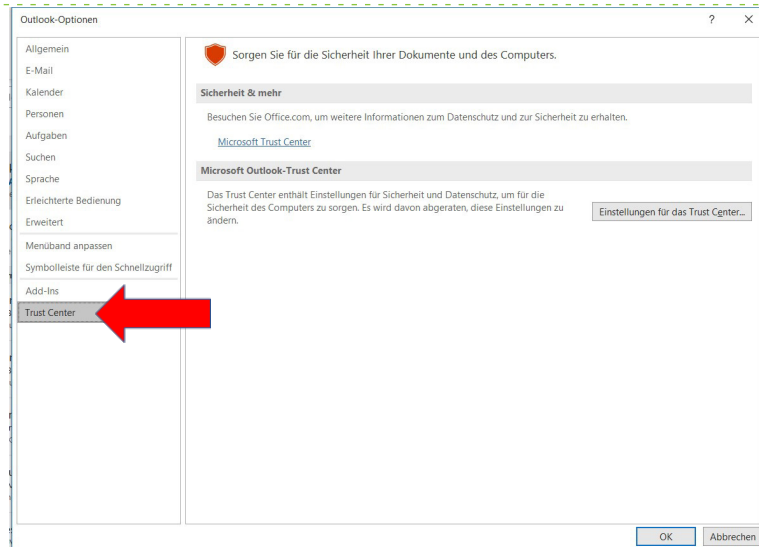
Schritt 1

Starten Sie Outlook
Wechseln Sie vom Post-
eingang nach -> Datei ->
Optionen



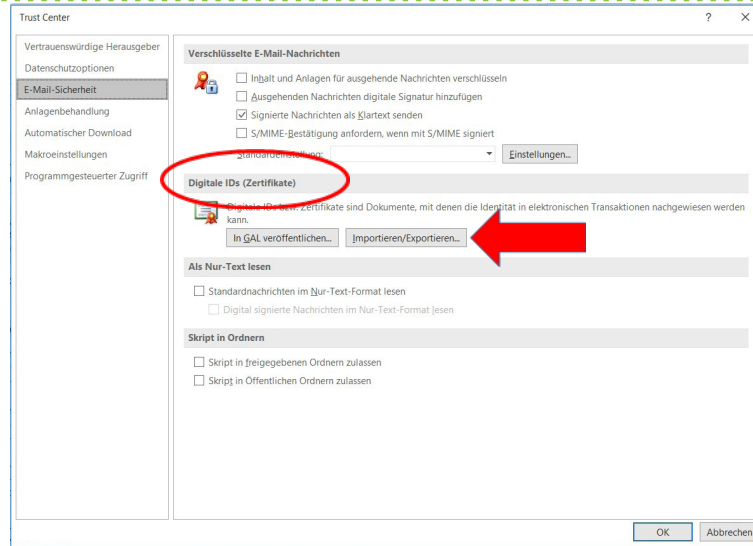
Schritt 2

Und klicken Sie dann auf
Trust Center und anschlie-
ßend Einstellungen für des
Trust Center



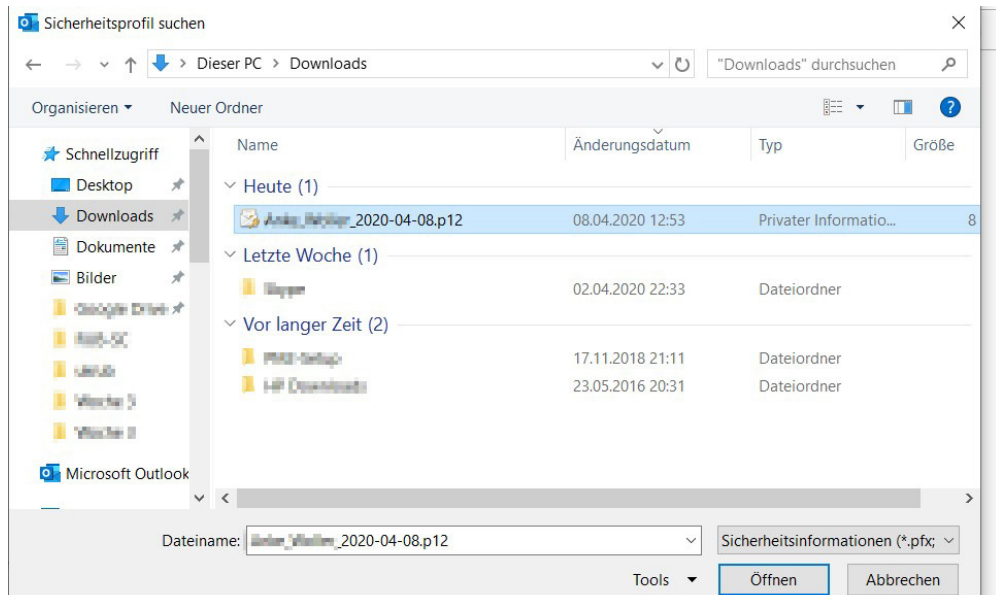
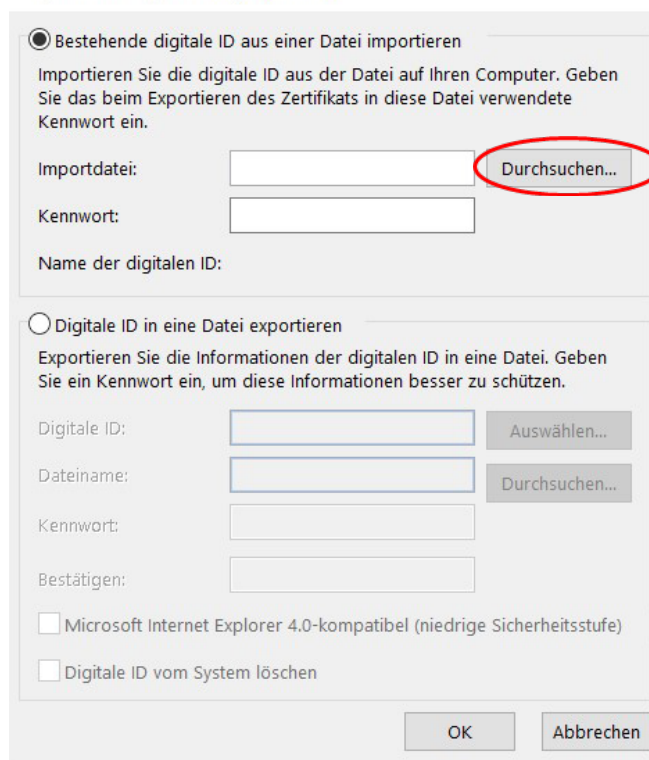
Schritt 3

Nachdem Auswählen von E-Mail Sicherheit klicken Sie unter „Digitale IDs (Zertifikate)“ auf Importieren/Exportieren

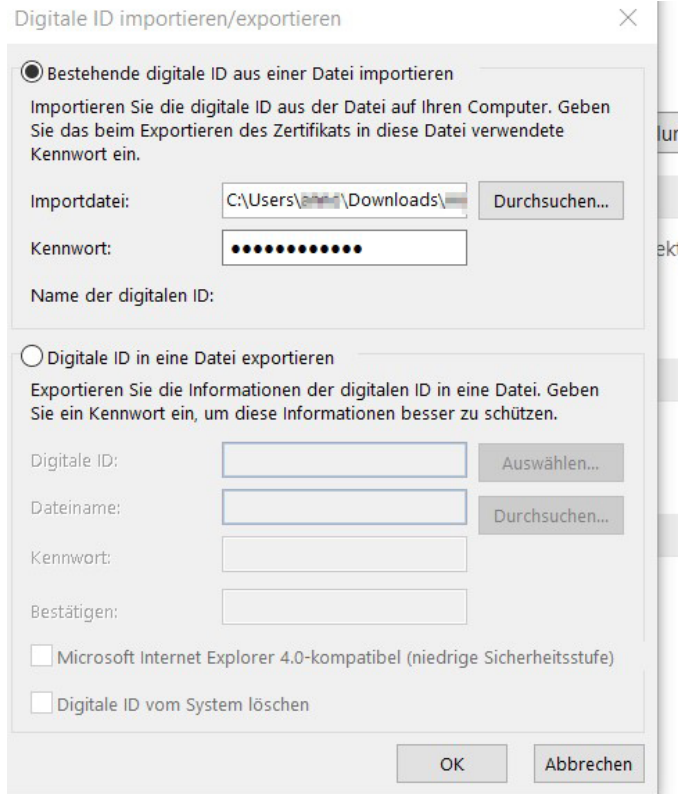


Über Durchsuchen können Sie nach Ihrer *.p12 suchen und sie auswählen.

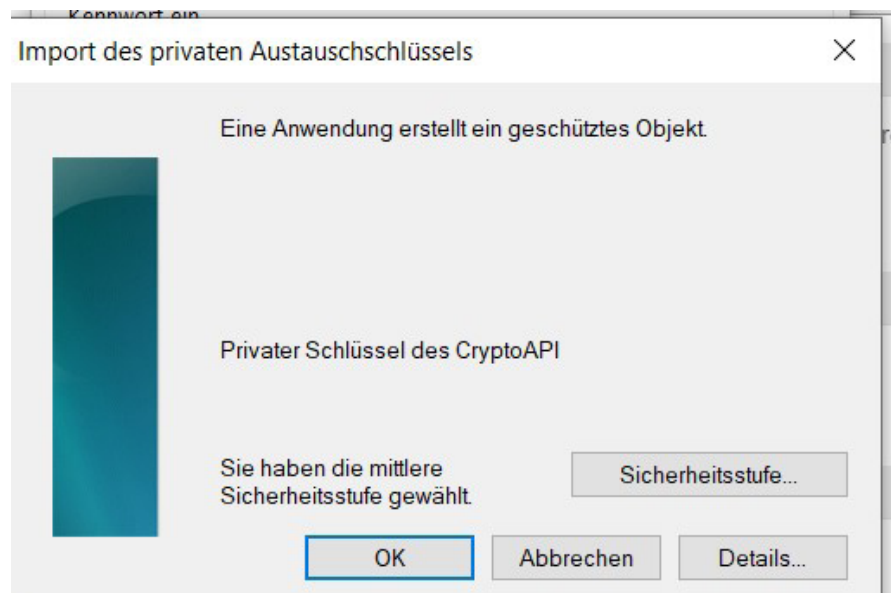
Digitale ID importieren/exportieren



Geben Sie das von Ihnen gewählte Passwort ein und klicken Sie auf OK, um die Datei zu importieren.



Wählen Sie die gewünschte Sicherheitsstufe aus und bestätigen Sie das mit OK. Die Einstellung können Sie später wieder ändern.

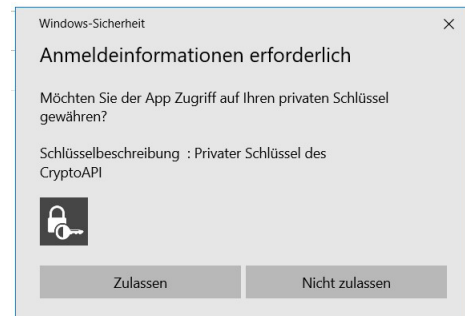
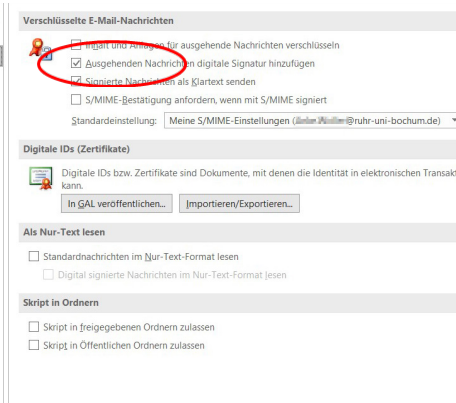


Schritt 4

Als letzten Schritt müssen Sie noch einschalten, dass den Ausgehenden Mails das Zertifikat angehängt werden.

Schließen Sie alle Fenster, indem Sie mit OK bestätigen.

Ab jetzt werden die Mails mit Zertifikat verschickt und Sie erhalten folgende Nachricht darüber, die Sie zulassen müssen.



Bei Fragen & Problemen

Bei Fragen und Problemen können Sie sich an unseren Helpdesk wenden: its-helpdesk@ruhr-uni-bochum.de.