

# Handout

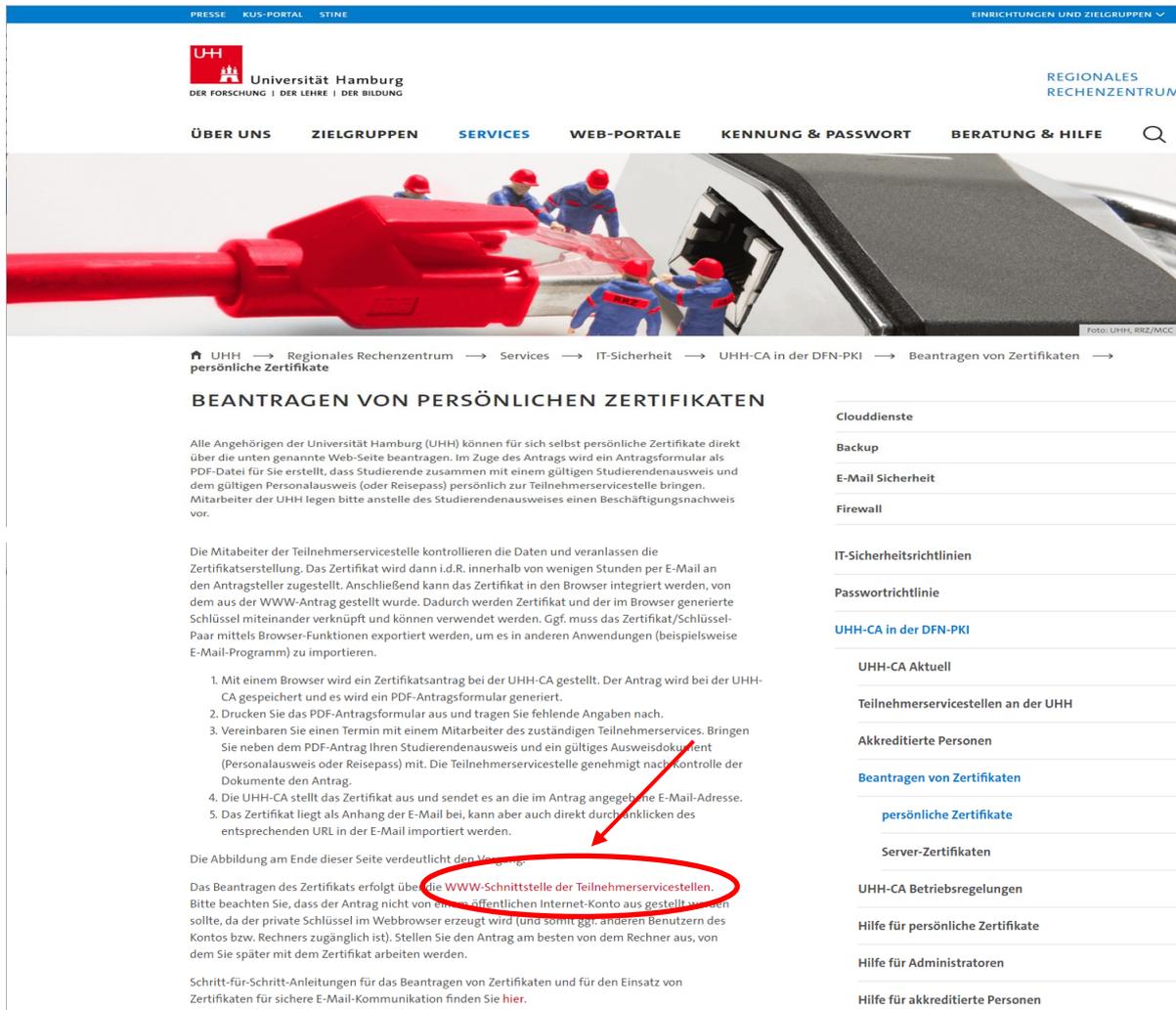
## für die Beantragung eines persönlichen Zertifikats

### Hinweis:

Für die Beantragung ist die Installation des Firefox Webbrowsers erforderlich! Wenn nicht schon vorhanden können Sie sich den Browser im RRZ Service Portal shoppen:

<https://rrz-serviceportal.uni-hamburg.de>

- Im ersten Schritt muss ein persönliches Zertifikat auf den Seiten des RRZ beantragt werden: <https://www.rrz.uni-hamburg.de/services/sicherheit/pki/beantragen-von-zertifikaten/persoenele-zertifikate.html>
- Bitte klicken Sie dann auf „WWW-Schnittstelle der Teilnehmerservicestellen“.



The screenshot shows the website navigation for requesting personal certificates. The breadcrumb trail is: UHH → Regionales Rechenzentrum → Services → IT-Sicherheit → UHH-CA in der DFN-PKI → Beantragen von Zertifikaten → persönliche Zertifikate. The main heading is 'BEANTRAGEN VON PERSÖNLICHEN ZERTIFIKATEN'. The text explains that employees can request certificates directly via the website, which generates a PDF form. It lists steps: 1. Request form, 2. Print and fill, 3. Bring to service desk with ID and passport, 4. UHH-CA sends certificate to email, 5. Import certificate. A red circle highlights the link 'die WWW-Schnittstelle der Teilnehmerservicestellen' in the text, with an arrow pointing to the 'persönliche Zertifikate' link in the right-hand navigation menu.

- Auf der neuen Seite suchen Sie sich Ihre Teilnehmerservicestelle heraus, die für Sie zuständig ist und klicken bitte auf „Webformular für Anträge an die Teilnehmerservicestelle...“ (Im Beispiel unten die Teilnehmerservicestelle am RRZ)

UHH → Regionales Rechenzentrum → Services → IT-Sicherheit → Zertifikate → Teilnehmerservicestellen an der UHH

## TEILNEHMERSERVICESTELLEN AN DER UHH

Das persönliche Erscheinen für ein Nutzer- oder Serverzertifikat ist nicht mehr erforderlich. Die Legitimation findet durch die Eingabe der B-Kennung und Passwort im Webformular statt.

Die folgenden Teilnehmerservicestellen (auch Registrierungsstellen genannt) sind bisher an der UHH eingerichtet:

### Teilnehmerservicestelle am RRZ

Die Teilnehmerservicestelle am RRZ bearbeitet nur diejenigen Zertifikate die nicht von einer der weiter unten genannten Teilnehmerservicestellen bearbeitet werden.

Beantragen Sie ein Nutzerzertifikat bitte über die folgende Webseite:

- [Webformular des CERT-Managers von SECTIGO für Nutzerzertifikatsanträge an die Teilnehmerservicestelle am RRZ](#)

Beantragen Sie ein Gruppenzertifikat bitte über das Webformular:

- [Webformular zur Beantragung eines Gruppenzertifikats](#)

Beantragen Sie ein Serverzertifikat bitte über die folgende Webseite:

- [Webformular des CERT-Managers von SECTIGO für Serverzertifikatsanträge an die Teilnehmerservicestelle am RRZ](#)

Die Teilnehmerservicestellen am RRZ sind für die folgenden Zertifikatsanträge zuständig:

- Neuer Link: <https://cert-manager.com/customer/DFN/idp/clientgeant>
- Auf der Webseite geben Sie bitte bei „Find Your Institution“ **Universität Hamburg** ein, dann sollte u.s. im Fenster eine Auswahl erscheinen und Sie klicken bitte auf „Universität Hamburg (UHH)“

Backup

Anti Virus

E-Mail Sicherheit

Firewall

IT-Sicherheitsrichtlinien

Passwortrichtlinie

Sperrlisten-Management

Zertifikate

UHH-CA Aktuell

[Teilnehmerservicestellen an der UHH](#)

Beantragen von Zertifikaten

[UHH-CA Betriebsregelungen](#)

The screenshot shows a web browser window with the URL <https://service.seamlessaccess.org/ds/?entityID=https%3A%2F%2Fcert-manager.com%2Fshibboleth&return=https%3A%2F%2Fcert-manager.com%2Fshibboleth>. The page title is "Sectigo Certificate Manager". The main content area features a "Find Your Institution" search box with the text "Your university, organization or company". The search input field contains "Universität Hamburg". Below the search box, there are examples: "Science Institute, Lee@uni.edu, UCLA". A checkbox labeled "Remember this choice" is checked, and a "Learn More" link is present. The search results list "HafenCity Universität Hamburg" with the email "hcu-hamburg.de". Below that, "Universität Hamburg (UHH)" is listed with the email "uni-hamburg.de". Red arrows in the original image point to the search input field and the "Universität Hamburg (UHH)" result.

- Im neuen Fenster geben Sie bitte Ihre Benutzerkennung und Ihr dazugehöriges Passwort ein und klicken bitte auf „LOGIN“
- Wenn das UHH-Login schon ausgeführt wurde aufgrund irgendwelcher Anmeldungen, erscheint dieses Fenster nicht!

Web Anmeldedienst

https://login.uni-hamburg.de/idp/profile/SAML2/Redirect/SSO?execution=e1s1

**Universität Hamburg**  
DER FORSCHUNG | DER LEHRE | DER BILDUNG

## UHH-LOGIN

Ihre Benutzerkennung, z.B. BAO1234  
baq2927

Passwort  
.....

**Öffentlicher PC**  
 Ich arbeite an einem öffentlich zugänglichen Computer

**Revoke consent**  
 Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

**LOGIN**

**Login-Hinweis**  
Das UHH-Login ermöglicht Ihnen den Zugang zu unter anderem folgenden Diensten:

- KUS-Portal (Intranet)  
Das KUS bietet Beschäftigten der Universität Informationen und Formulare zu allen Leistungen der Universitätsverwaltung. Den öffentlich zugänglichen Bereich der Verwaltung finden Sie hier.
- SharePoint

Sie müssen sich nur einmal am Tag anmelden, um alle Dienste nutzen zu können (Single Sign-on). Zur Authentifizierung wird die Software Shibboleth genutzt.

Bitte beachten Sie, dass bei der Anmeldung von einem öffentlich zugänglichen Computer bestimmte Funktionen nicht zur Verfügung stehen.

- Im folgenden Fenster sollten Ihre Daten auch schon ausgefüllt sein und Sie klicken bitte auf „Certificate Profile\*“

SECTIGO

## Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name **Wagner, Nicolai**

Organization **Universität Hamburg**

Email **Nicolai.Wagner@uni-hamburg.de**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*

- Im Auswahlfenster klicken Sie bitte im Feld „Certificate Profile“ auf „GÉANT Personal email signing and encryption“

**SECTIGO**

### Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name **B**  
Organization **Universität Hamburg**  
Email **i@uni-hamburg.de**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*  
GÉANT Personal email signing and encryption

GÉANT Personal email signing and encryption

(but not sign PDF documents).

- Im Feld „Term“ klicken Sie bitte auf „730 days“

**SECTIGO**

### Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name **B**  
Organization **Universität Hamburg**  
Email **i@uni-hamburg.de**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*  
GÉANT Personal email signing and encryption

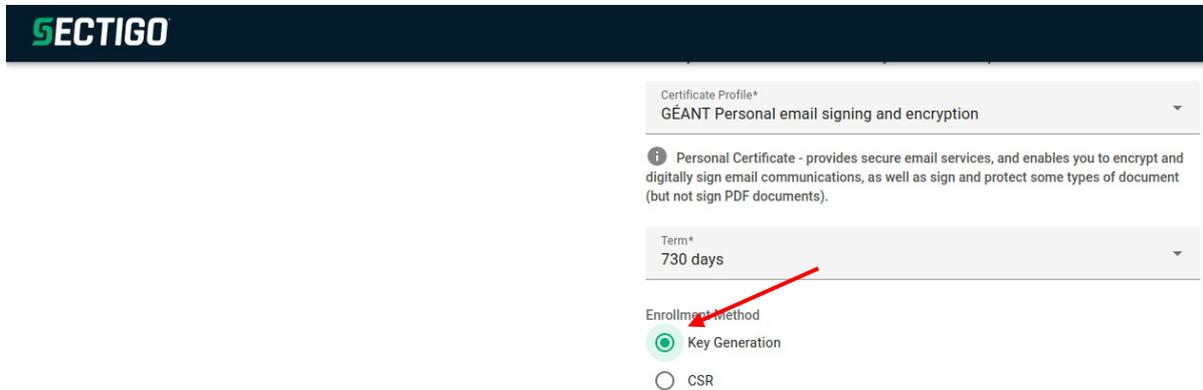
 Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).

Term\*

365 days

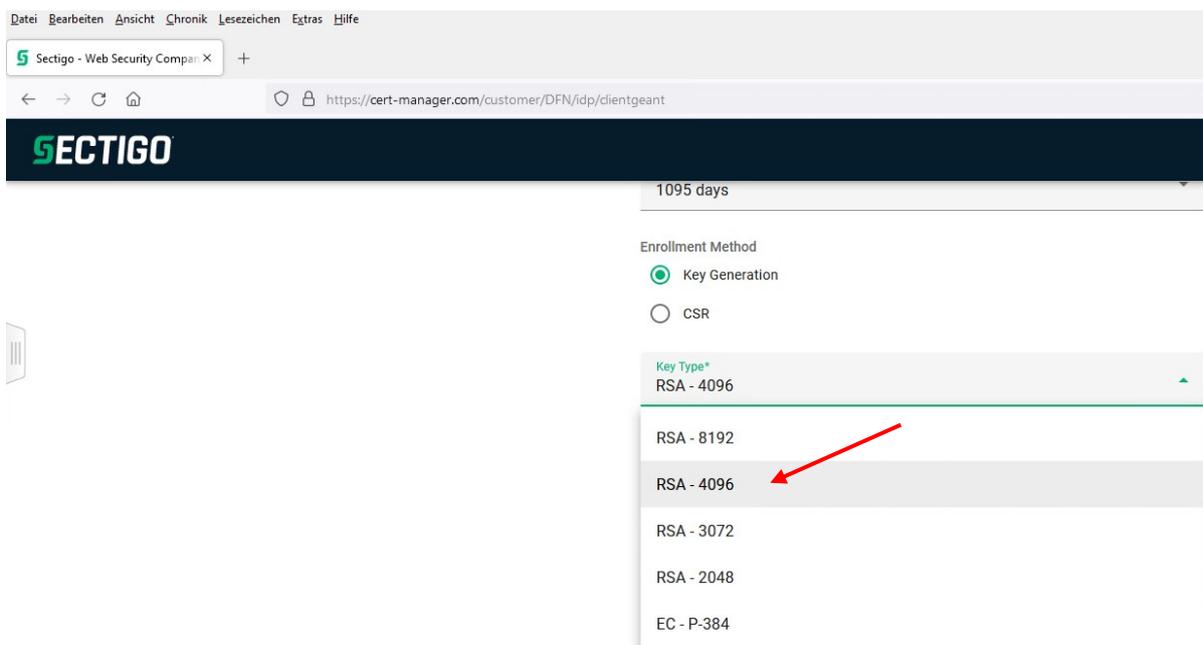
730 days

- Im Feld „Enrollment Method“ klicken Sie bitte auf „Key Generation“



The screenshot shows the Sectigo web interface. At the top, there is a dark blue header with the Sectigo logo. Below the header, there is a form with several fields. The 'Certificate Profile\*' dropdown is set to 'GÉANT Personal email signing and encryption'. Below it, there is an information icon and a description: 'Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents)'. The 'Term\*' dropdown is set to '730 days'. The 'Enrollment Method' section has two radio buttons: 'Key Generation' (which is selected) and 'CSR'. A red arrow points to the 'Key Generation' radio button.

- Im Feld „Key Type“ klicken Sie bitte auf „RSA – 4096“



The screenshot shows the Sectigo web interface. At the top, there is a dark blue header with the Sectigo logo. Below the header, there is a form with several fields. The 'Term\*' dropdown is set to '1095 days'. The 'Enrollment Method' section has two radio buttons: 'Key Generation' (which is selected) and 'CSR'. The 'Key Type\*' dropdown is open, showing a list of options: 'RSA - 4096', 'RSA - 8192', 'RSA - 3072', 'RSA - 2048', and 'EC - P-384'. The 'RSA - 4096' option is highlighted, and a red arrow points to it.

- In den Feldern **1 und 2** „Password“ geben Sie ein möglichst komplexes Passwort ein.
- Bitte beachten Sie dabei, dass die folgenden Sonderzeichen **NICHT** erlaubt sind: § °

Password is required to unlock the certificate file download to protect private key.

Password\*   

Password Confirmation\*   

Choose key protection algorithm.

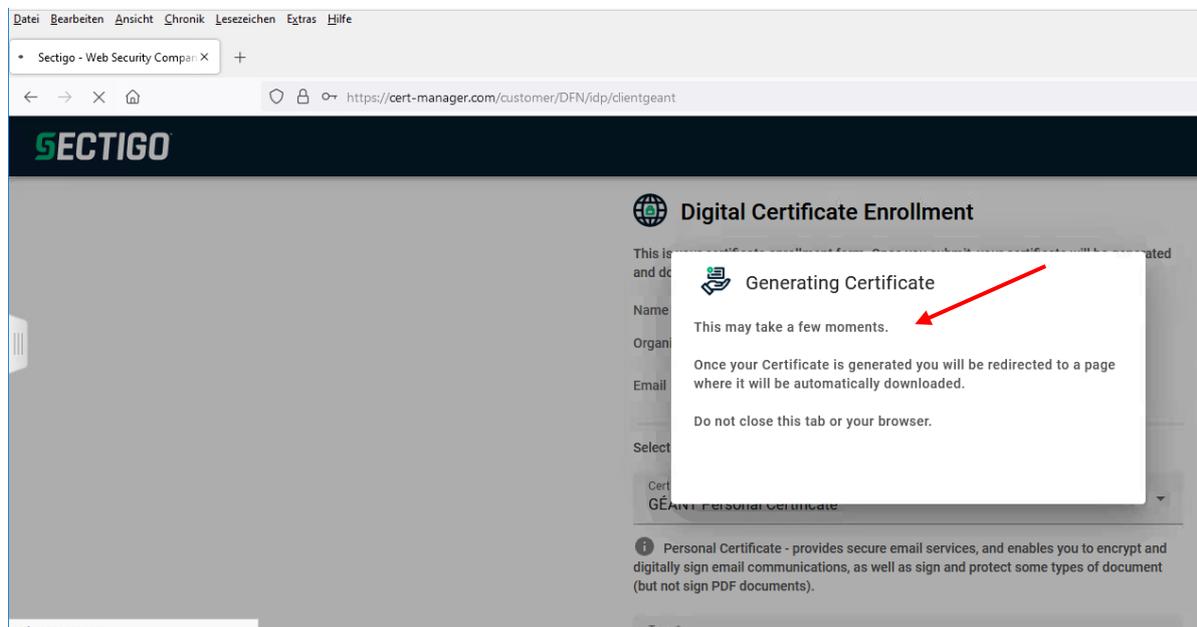
Algorithm  
Compatible TripleDES-SHA1

[I have read and agree to the terms of the EULA](#)

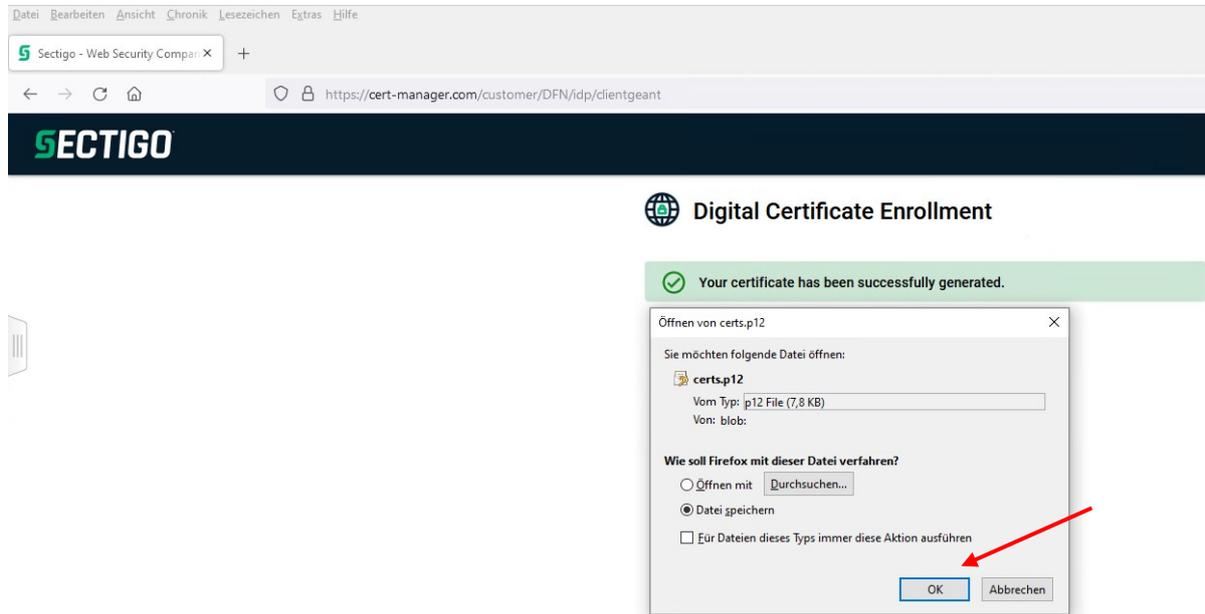
Submit

- Nach dem Setzen des Passworts wählen Sie unbedingt **„Compatible TripleDES-SHA1“** aus.
- Danach setzen bitte den Haken, klicken im neuen Fenster auf **„Agree“** und klicken dann auf **„Submit“**

- Das kann jetzt etwas dauern (auch mehrere Minuten), bitte Fenster **NICHT** schließen!



- Ihr persönliches Zertifikat wurde jetzt erstellt und Sie speichern die Datei.



- Damit ist Ihr Zertifikat gespeichert und Sie können es jetzt weiterverwenden für den Import in Outlook  
<https://www.rrz.uni-hamburg.de/services/e-mail/fuer-mitarbeiter/exchange/handouts/handout-einbindung-eines-persoentlichen-zertifikats-in-outlook.pdf>