Nutzerzertifikat beantragen

Inhalt der Seite

WICHTIG!

Diese Anleitung beschreibt, wie Sie ein Nutzerzertifikat für Ihre **persönliche E-Mail-Adresse** b eantragen können. Wenn Sie ein Zertifikat für eine **Funktions-E-Mail-Adresse** beantragen möchten, folgen Sie bitte der Anleitung für Gruppenzertifikate.

Wenn Sie Ihre **E-Mails signieren und/oder verschlüsseln** oder Ihre **PDFs signieren/unterschreiben** möchten, benötigen Sie ein Nutzerzertifikat.

- Das Zertifikat ist nur für eine Mailadresse gültig und wird Ihnen auf Ihre **Hauptmailadresse** ausgestellt.
- Weicht die Mailadresse des Absenders und des Zertifikats voneinander ab, wird dem Empfänger eine Warnung angezeigt! **Dies ist unbedingt zu vermeiden!**
- Sie können **fünf Zertifikate** gleichzeitig besitzen. Sobald Sie ein sechstes erstellen, wird das älteste automatisch gelöscht.

Kennen Sie ihre Hauptmailadresse nicht?

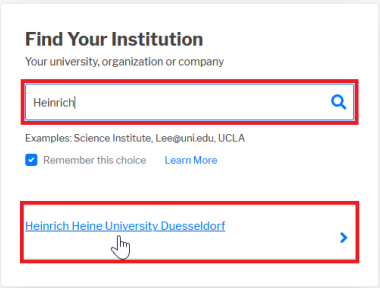
Prüfen Sie Ihre Hauptmailadresse: Schicken Sie sich selbst eine Mail zu. Alternativ loggen Sie sich im IDM (idm.hhu.de) ein und prüfen Ihre Einstellung unter "Mein Profil" "EMail".

Ändern Sie ggf. Ihre Haupt-Mailadresse im IDM und folgen dafür dieser Anleitung.

Läuft Ihr Zertifikat ab?

Es besteht **keine Möglichkeit zur Verlängerung** des Zertifikates. Sie müssen (vor Ablauf des alten) ein neues Zertifikat beantragen. Weitere Informationen finden Sie weiter unten auf dieser Seite.

Anleitung: Nutzerzertifikat beantragen



1. Klicken Sie auf folgenden Link, um auf die Seite von **Sectigo** zu gelangen: **Nutzerzertifikat beantragen**

2. Wählen Sie die HHU aus, indem Sie im Suchfeld "HHU", "Heinrich" o.ä. eingeben. Im unteren Teil wird Ihnen unsere Einrichtung angeboten. Mit Klick auf das Feld **„Heinrich Heine University Duesseldorf“** werden Sie zur Anmeldung weitergeleitet.

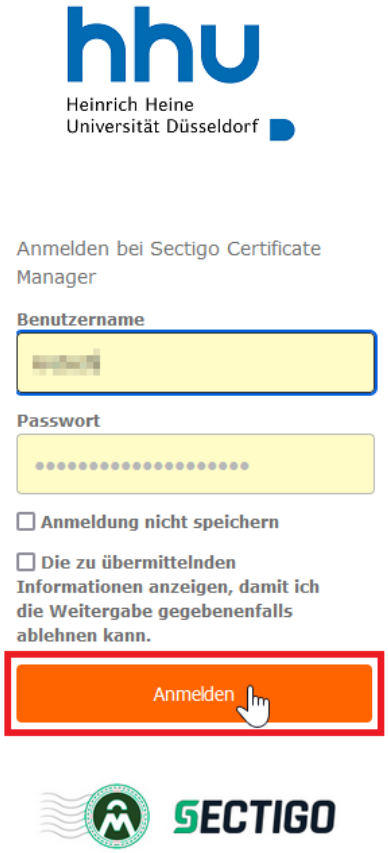
---

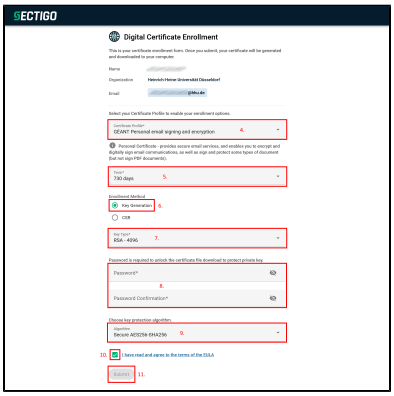
3. Im Anmeldefenster tragen Sie unter Benutzername Ihre **Uni-Kennung** und das dazugehörige **Passwort** ein und klicken anschließend auf **„Anmelden“**.

Es werden Ihnen nun die an Sectigo übermittelten Attribute angezeigt:

- Ihr Name
- Mailadresse
- Einrichtung von der aus Sie sich anmelden (in Ihrem Fall: HHU Düsseldorf).v

Diese Informationen werden benötigt, um das Zertifikat Ihrer Person und Mailadresse zuzuordnen. Mit Klick auf **„Akzeptieren“** werden Sie weitergeleitet.





4. Ihnen wird nun angezeigt, für wen das Zertifikat ausgestellt wird, zu welcher Einrichtung Sie gehören und für welche Mailadresse das Zertifikat gültig sein wird. Wählen Sie zunächst das **Zertifikatsprofil** ("Certificate Profile") aus. Wählen Sie für den **Versand von signierten und verschlüsselten E-Mails** bzw. zum **Signieren und Unterschreiben von PDFs** das **„Géant Personal email signing and encryption“**.

> **Hinweis**
>
> *"... (but not sign PDF documents)"* Damit Adobe Reader Ihr Nutzerzertifikat als vertrauenswürdig einstuft, müssen zuvor spezielle Einstellungen getroffen werden.
>
> Mit diesen Anleitungen ist das **Signieren** von PDFs und das **Prüfen** von diesen möglich.

5. Unter „Term“ legen Sie die **Gültigkeitsdauer** des Zertifikats fest. Hier stehen 1, 2 oder 3 Jahre ("365 days", "730 days") zur Auswahl. Sobald Sie den Zeitraum ausgewählt haben, erscheinen die letzten auszufüllenden Felder.

6. Bei der Methode können Sie entscheiden, ob Sie einen neuen Schlüssel **„Key Generation“** generieren **oder** einen bereits erstellten Request hochladen **„CSR“*** .

In den meisten Fällen sollten Sie "**Key Generation**" wählen.

Alternativ können Sie auch selbst einen Request bzw. CSR erstellen. Wie das geht, erfahren Sie hier: **CSR erstellen**

Key Generation:

7. Unter „Key Type“ können Sie zwischen **RSA** und **EC-P** in **verschiedenen Schlüssellängen** wählen. **Wir empfehlen: RSA-4096**

> **Hinweis**
>
> Zertifikate mit den ECC-Schlüsseltypen P-384 und P-256 können nur für Signatur und Authentisierung, aber **nicht für Verschlüsselung** verwendet werden.
>
> Je höher die Schlüssellänge, desto schwieriger ist das Kompromittieren des Schlüssels. Allerdings steigt auch die Rechenleistung und damit die Zeit zum Ver- und Entschlüsseln.

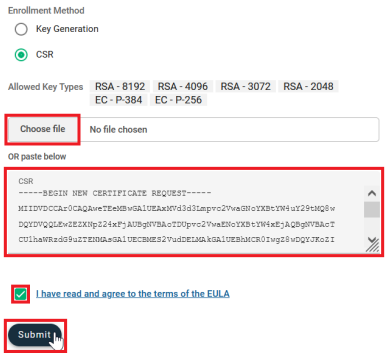
8. Vergeben Sie ein **Passwort**, um das **Zertifikat** zu **schützen** und zum **Öffnen nach** dem **Herunterladen** . Geben Sie das Passwort 2x ein.

9. Wählen Sie den Schutzalgorithmus: **"Secure AES256-SHA256"**, dieser ist modern und am sichersten.

> **Achtung**: Nicht alle Programme unterstützen allerdings diesen Standard, es kann zu Fehlern wie: „Das eingegebene Kennwort ist falsch.“, „Fehler im zugrunde liegenden Sicherheitssystem. Ungültigen Anbietertyp angegeben.“ kommen. In diesem Fall legen Sie bitte ein neues Zertifikat an und verwenden folgenden Algorithmus: "**Compatible TripleDES-SHA1**". Mehr Informationen gibt es hier: https://doku.tid.dfn.de/de:dfnpki:tcs:usercert#auswahl_des_key_protection_algorithms_in_formularen_fuer_p12-dateien

10. Um die EULA (End User License Agreement) zu akzeptieren, setzen Sie den entsprechenden Haken.

11. Mit Klick auf **„Submit“** schicken Sie die Anfrage ab. Zum Abschluss sollte Ihnen die Nachricht *"Your certificate has been successfully generated"* angezeigt und das Zertifikat (mit dem Namen *certs.p12*) zum **Download** angeboten werden. Speichern Sie das Zertifikat an einem beliebigen Ort wo Sie es wiederfinden.



***Alternative: CSR hochladen**

1. Laden Sie Ihren zuvor erstellten Request hoch („Choose File“) **oder** kopieren Sie ihn mittels Copy & Paste in das Eingabefeld („paste below“). Damit sind alle Eingaben vollständig.

2. Um die EULA (End User License Agreement) zu akzeptieren, setzen Sie den entsprechenden Haken.

3. Mit Klick auf **„Submit“** schicken Sie die Anfrage ab. Zum Abschluss sollte Ihnen die Nachricht *"Your certificate has been successfully generated"* angezeigt und das Zertifikat (mit dem Namen *certs.p12*) zum **Download** angeboten werden. Speichern Sie das Zertifikat an einem beliebigen Ort wo Sie es wiederfinden. Sie erhalten das Zertifikat **nicht** zusätzlich per Mail.

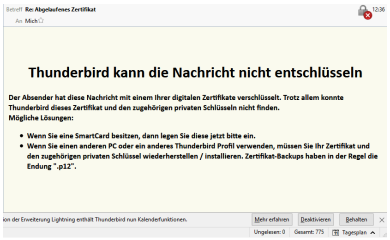
Hinweise zur Erneuerung des Nutzerzertifikats

Jedes Zertifikat hat eine begrenze Gültigkeitsdauer, nach deren Überschreiten es nicht mehr zum Signieren oder Verschlüsseln verwendet werden kann. Das Start- und Ablaufdatum kann im Zertifikatsspeicher des Betriebssystems oder der Mail-Software eingesehen werden. Jeder Zertifikatseigentümer ist eigenverantwortlich dafür, vor dem Erreichen des Ablaufdatums seine Zertifikate zu erneuern.

Prinzipiell ist dabei genau wie beim Beantragen des ersten Nutzerzertifikates entsprechend der Anleitungen vorzugehen. Bei der Konfiguration des E-Mail-Clients ist darauf zu achten, dass auch wirklich nur das neue Zertifikat für E-Mail-Signierung und Verschlüsselung ausgewählt wird, da auch das alte Zertifikat weiterhin zur Auswahl steht. Finden Sie hier eine Anleitung zur Auswahl des Zertifikates in Outlook.

Das alte Zertifikat inkl. zugehörigem privatem Schlüssel kann beliebig lange parallel zum neuen im Zertifikatsspeicher gehalten werden. Ein endgültiges Löschen aus dem Speicher empfiehlt sich erst, wenn das Zertifikat bereits einige Zeit abgelaufen ist und auch **keinesfalls mehr zum Entschlüsseln von bereits erhaltenen E-Mails** (oder andere Dateien) **benötigt wird. Nach einem Löschen ist dies nicht mehr möglich.**

Sie benötigen abgelaufene Zertifikate weiterhin, um ältere verschlüsselte E-Mails in Ihrem Posteingang lesen zu können.



Dies gewährleisten Sie, indem sich beide Zertifikate im Zertifikatsspeicher befinden.

Wie das neue Zertifikat in die jeweiligen Clients eingebunden wird, können Sie aus den Anleitungen "Nutzerzertifikate in Mailprogramme einbinden" entnehmen. Im letzteren Abschnitt der jeweiligen Anleitungen wird das Auswechseln des Zertifikats beschrieben.