# Applying for a User Certificate (English Version)

If you want to **sign or encode your personal e-mails or your PDFs**, you need a User Certificate.

- The certificate is valid for one e-mail address only and is edited for your **main e-mail address** at the HHU.
- If the e-mail addresses of the sender and of the certificate are different, the recipient gets a warning notice. This should be avoided.
- You can own **5 certificates** at the same time. As soon as you create a sixth certificate, the oldest one will automatically be deleted.

**Overview**



**You don’t know your main e-mail address?**

Log in at the IDM (idm.hhu.de) and check your main mail address at "My Profile"  "EMail".

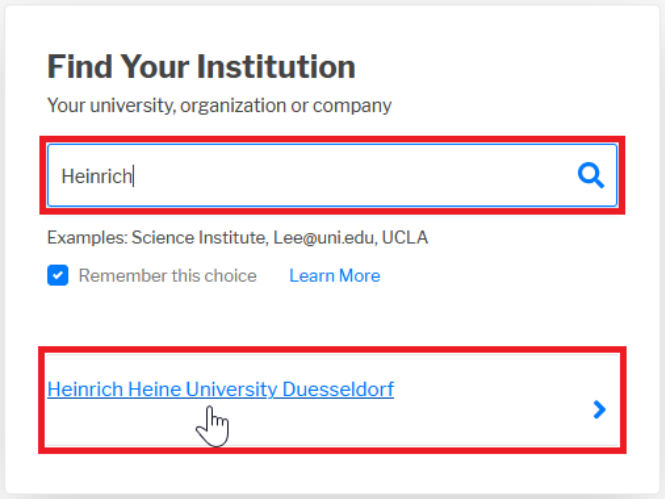
To change your main e-mail address, follow this instruction.

**Your Certificate expires?**

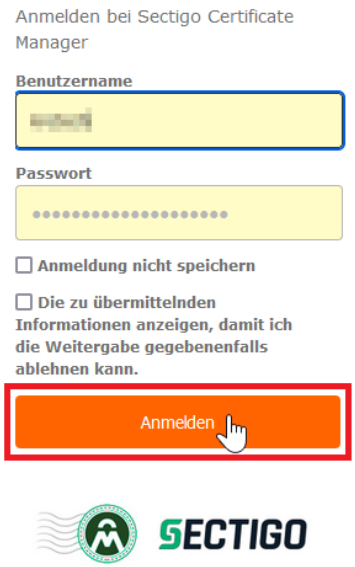
There’s **no possibility to prolong** the certificate. You have to apply for a **new one** (before the old one expires). Further information you find lower on this page.

Instruction: Apply for a User Certificate

Click on the following Link to get on the **Sectigo** page: **Applying for User Certificate**




Choose the HHU by inserting "HHU", "Heinrich" or similar into the search box. By clicking on **„Heinrich Heine University Duesseldorf“**you are led further to the Login window.




In the Login window, you put in your **university ID** as user name and the according **password**. Then click on **„Anmelden“**.

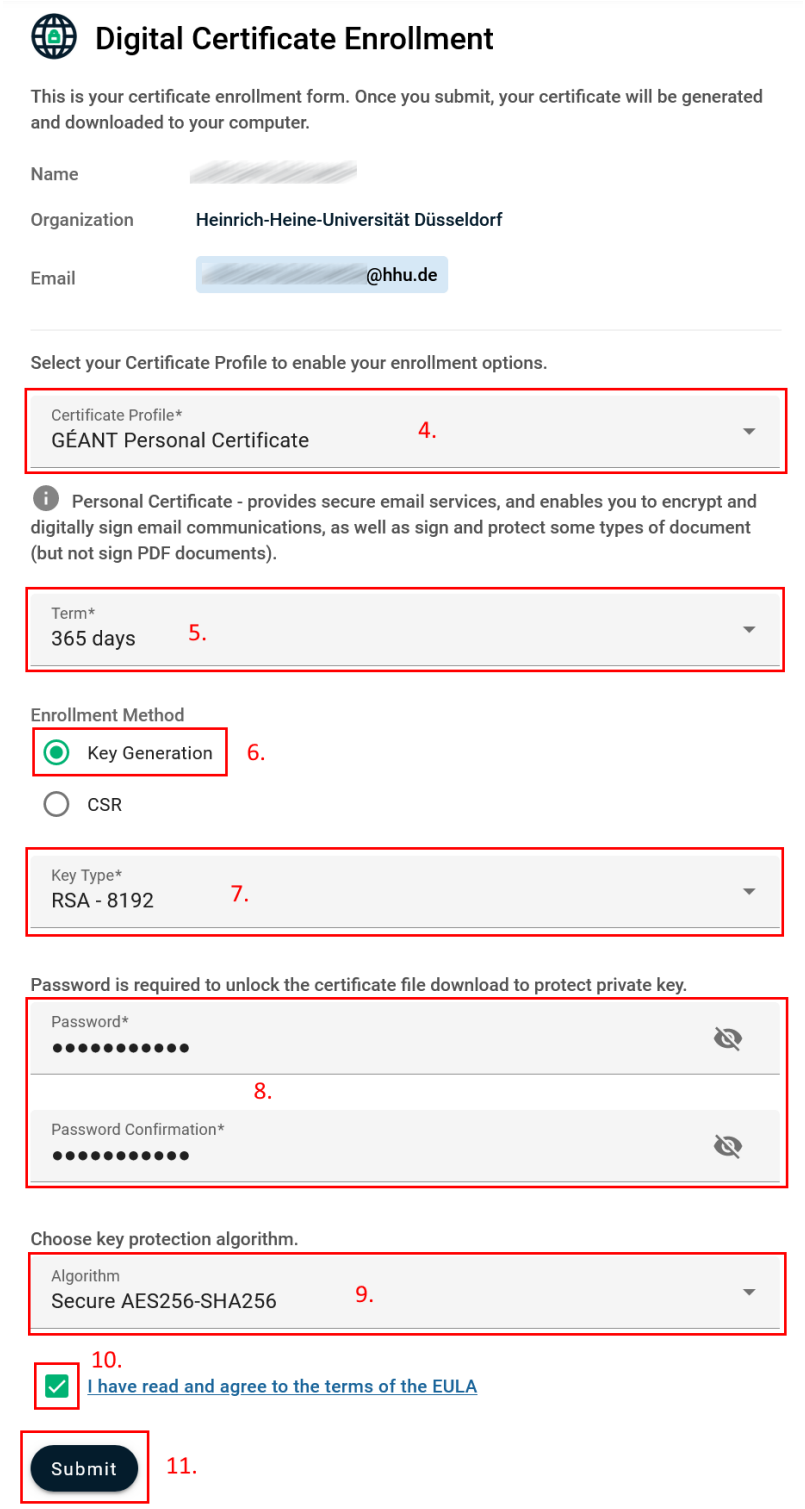
Now the attributes that are delivered to Sectigo are listed:

- Your name
- Mail address
- Institution (here: HHU Düsseldorf).

These Informations are needed to assign the certificate to your person and e-mail address. By clicking on **„Accept“** you are directed further.

Now there is shown the name the certificate is issued for, the institution you belong to, and the e-mail address the certificate is valid for. Choose now the **C ertificate Profile**. For the **distribution of signed and encoded e-mails** and the **signing of PDFs** the **„Géant Personal Certificate“**.

**(Notice:** *"... (but not sign PDF documents)"* For Adobe Reader there have to be made additional settings.




As „Term“you set the **Validity period**of the certificate: 1, 2 or 3 years ("365 days", "730 days", "1095 days").

As Enrollment Method you can decide between generating a new key **„Key Generation“or**uploading an already existing Request **„CSR“***.

In most cases you should choose "**Key Generation**".

Alternatively you may create a Request / CSR: **Create CSR**

After setting this information, the whole remaining form can be seen.

**Key Generation:**

Under „Key Type“ you may choose between **RSA**and **EC-P**in **different Key lengths**. **We recommend: RSA-4096**

**Notice:**

Certificates with the ECC Key Types P-384 and P-256 can only be used for Signature and Authentication, but **not for encryption**.

Choose a **Password** to **protect** the **Certificate**and to open it **after Downloading it**. Confirm your Password.

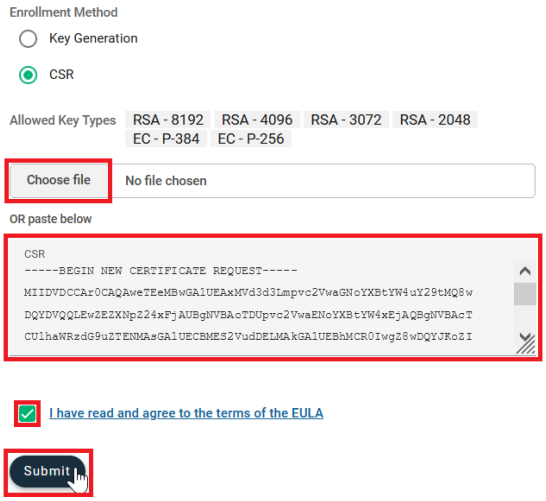
Choose the Protection Algorithm: **"Secure AES256-SHA256"**, the most modern secure one.

**Attention**: Not all the programs support this standard, there may be issues like: „Das eingegebene Kennwort ist falsch.“, „Fehler im zugrunde liegenden Sicherheitssystem. Ungültigen Anbietertyp angegeben.“ In this case please set up a new certificate with the algorithm: "**Compatible TripleDES-SHA1**". More Information you find here: https://doku.tid.dfn.de/de:dfnpki:tcsfaq#auswahl_des_verschluesselungsalgorithmus_fuer_p12-dateien_pkcs_12

To accept the EULA (End User License Agreement), set the according mark.

Click on **„Submit“**. After that you get the notice *"Your certificate has been successfully generated"* and the certificate (named *certs.p12*) for **Download**. Store the Certificate in a file where you easily find it again.

***Alternative: CSR upload**




1. Upload your previosly generated Request („Choose File“) **or** copy it by Copy & Paste into the input box ( „paste below“). Now your informations are complete.
2. Set the mark to accept the EULA (End User License Agreement).
3. Click on **„Submit“**. After that you get the notice *"Your certificate has been successfully generated"* and the certificate (named *certs.p12*) for **Dow nload**. Store the Certificate in a file where you easily find it again. You don’t receive the Certificate additional per Mail.

Please keep older Certificates stored because you might need them to open older files.