

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

- [Instructions: Applying for a User Certificate](#)
- [Hints for Renewal of User Certificates](#)

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](#)

Find Your Institution
Your university, organization or company

Heinrich| 🔍

Examples: Science Institute, Lee@uni.edu, UCLA

Remember this choice [Learn More](#)

Heinrich Heine University Duesseldorf >

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.

Anmelden bei Sectigo Certificate
Manager

Benutzername

Passwort

Anmeldung nicht speichern

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



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 **Certificate 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](#).



Digital Certificate Enrollment

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

Name

Organization **Heinrich-Heine-Universität Düsseldorf**

Email @hhu.de

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*
GÉANT Personal Certificate 4.

i 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 5.

Enrollment Method

Key Generation 6.

CSR

Key Type*
RSA - 8192 7.

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

Password*
●●●●●●●●

8.

Password Confirmation*
●●●●●●●●

Choose key protection algorithm.

Algorithm
Secure AES256-SHA256 9.

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

11.

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**“oruploading 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-Pin** 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

Enrollment Method

- Key Generation
 CSR

Allowed Key Types **RSA - 8192** **RSA - 4096** **RSA - 3072** **RSA - 2048**
EC - P-384 **EC - P-256**

Choose file No file chosen

OR paste below

```
CSR
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVDCCAzOCAQAwTEeMBwGAIUEAxiMvd3d3Lmpvc2VwaGNoYXBtYW4uY29tMQ8w
DQYDVQQLEwZlZ2ZkZ24xZjAuYXBwLmVudDElMAkGA1UEBhMCFR0Iiw28wDQYJKoZI
CUIhARd9u2TENMAzGAIUECBMES2VudDElMAkGA1UEBhMCFR0Iiw28wDQYJKoZI
```

I have read and agree to the terms of the EULA

Submit

1. Upload your previously 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 **Download**. 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.