UNIVERSITÄT HOHENHEIM

Kommunikations-, Informations- und Medienzentrum (KIM)

Serverzertifikate

Bezug von SSL-Serverzertifikaten

Server certificates

Obtaining SSL server certificates

19.05.2025

kim.uni-hohenheim.de | kim-pki@uni-hohenheim.de

Inhalt

Voraussetzungen / *Prerequisites*

- Hohenheimer Benutzerkonto / *Hohenheim user account*
- FQDN des Servers (bspw. server.subdomain.uni-hohenheim.de) bzw. die Domain für Wildcardzertifikate (subdomain.uni-hohenheim.de) ist bekannt /
  FQDN of the server (e.g. server.subdomain.uni-hohenheim.de) or the domain for wildcard certificates (subdomain.uni-hohenheim.de) is known
- Der CSR ist bereits erstellt (falls noch nicht geschehen, hier die Erklärung: CSR erstellen) / *The CSR has already been created (if not already done, here is the explanation: Create CSR)*

CSR erstellen / Create CSR

CSR **C**ertificate **S**igning **R**equest

Zur Erstellung eines CSRs müssen Sie sich per SSH (bspw. Putty) und Ihrem Hohenheimer Benutzerkonto mit unserem Server login.uni-hohenheim.de verbinden. Sollten Sie keinen Zugriff auf unseren Server haben, schreiben Sie uns an kim-pki@uni-hohenheim.de. Wir werden Ihnen schnellstmöglich Zugriff gewähren.

To create a CSR, you must connect to our server login.uni-hohenheim.de via SSH (e.g. Putty) and your Hohenheim user account. If you do not have access to our server, please write to us at kim-pki@uni-hohenheim.de. We will grant you access as soon as possible.

Führen Sie nun unser Script certificateapplication.sh aus:
Now execute our script certificateapplication.sh:

```
[redacted]@login2:~> certificateapplication.sh
Servername (DNS name)
server.subdomain.uni-hohenheim.de
Organisation (Department of ...):
Universitaet Hohenheim (KIM (630))
Email:
kim-pki@uni-hohenheim.de
Add subjectAltNames? (NO|yes)
alternativeName.subdomain.uni-hohenheim.de
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = DE, ST = Baden-Wuerttemberg, L = Stuttgart, O =
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:a3:ee:05:bf:97:c7:c2:eb:52:f1:cc:24:c9:9b:
                    f7:b7:de:81:d8:0e:8e:75:8d:b8:b1:02:31:46:07:
                    95:e7:2a:82:4e:5c:97:b7:cf:b1:aa:d0:88:05:a1:
                    a7:b4:f9:52:f4:74:37:12:4f:16:0e:ee:14:e5:10:
                    cd:02:50:f1:1d:cf:aa:62:66:21:1c:a2:73:0c:1d:
```

Beispielangaben für die Erstellung eines CSR (Screenshot gekürzt)

Servername (DNS name): FQDN des Servers für den das Zertifikat beantragt wird. / *FQDN of the server for which the certificate is requested.*

Organisation (Department of …): im Regelfall „Universität Hohenheim“ / *usually "University of Hohenheim"*

Email: An diese Emailadresse wird das Zertifikat geschickt / *The certificate will be sent to this email address*

Add subjectAltNames?: Geben Sie hier „Yes“ oder „No“ ein. Je nachdem ob Sie noch einen alternativen/weiteren FQDN für den Server, für den das Zertifikat beantragt werden soll, im Zertifikat mit aufgenommen haben wollen. Wenn „Yes“ eingegeben wurde können Sie weitere FQDNs angeben. / *Enter "Yes" or "No" here. Depending on whether you want to include an alternative/additional FQDN for the server for which the certificate is to be requested in the certificate. If "Yes" was entered, you can enter additional FQDNs.*

Durch das Script wurde nun ein Schlüsselpaar erstellt. Mit dem privaten Schlüssel wurde zusätzlich ein CSR generiert. Der öffentliche Schlüssel und die im Script eingegebenen Infos sind im CSR enthalten. Der private Schlüssel wurde separat abgespeichert.
The script has now created a key pair. A CSR has also been generated with the private key. The public key and the information entered in the script are contained in the CSR. The private key was saved separately.

Die beiden Dateien (privater Schlüssel und CSR) finden Sie nun in Ihrem CIFS-Homeverzeichnis:
You will now find the two files (private key and CSR) in your CIFS home directory:

Windows:

\\campus.ad.uni-hohenheim.de\cifs\home\[Anfangsbuchstabe des HOH-Benutzerkontos]\[HOH-Benutzername]\[oben angegebener FQDN\
\\campus.ad.uni-hohenheim.de\cifs\home\[initial letter of the HOH user account]\[HOH user name]\[FQDN specified above

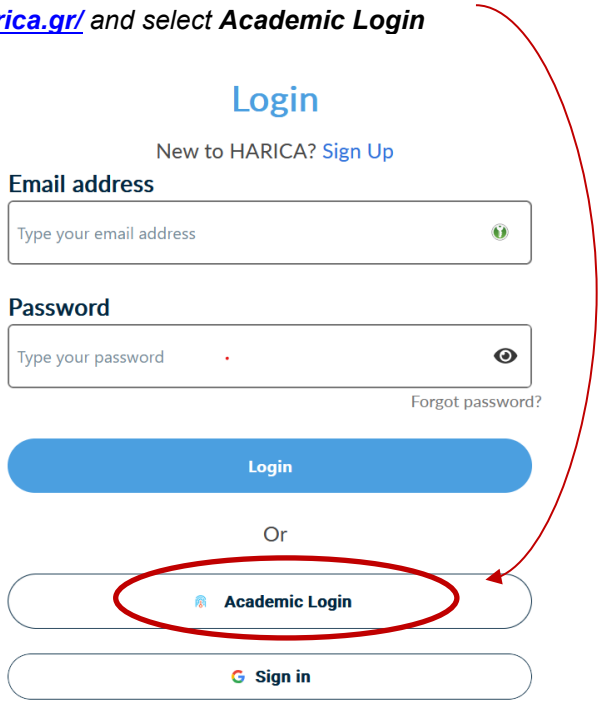
Linux (login.uni-hohenheim.de):
/home/[Anfangsbuchstabe des HOH-Benutzerkontos]/[HOH-Benutzername]/[oben angegebener FQDN/

Linux (login.uni-hohenheim.de):
/home/[initial letter of HOH user account]/[HOH user name]/[FQDN specified above/

Bezug des SSL-Serverzertifikats / Obtaining the SSL server certificate

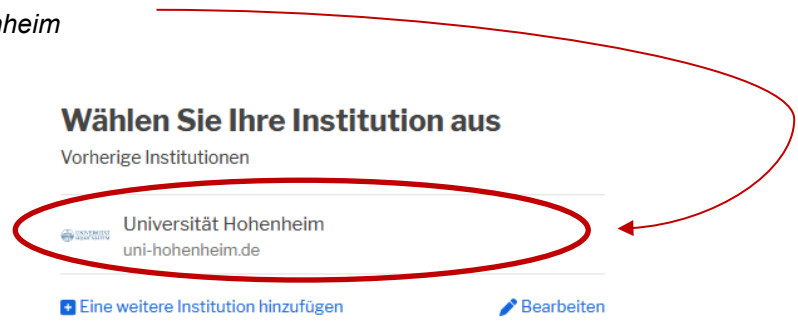
Rufen Sie die Website **https://cm.harica.gr/** auf und wählen Sie **Academic Login**

*Go to the website **https://cm.harica.gr/** and select **Academic Login***



Wählen Sie **Universität Hohenheim**

Choose University of Hohenheim

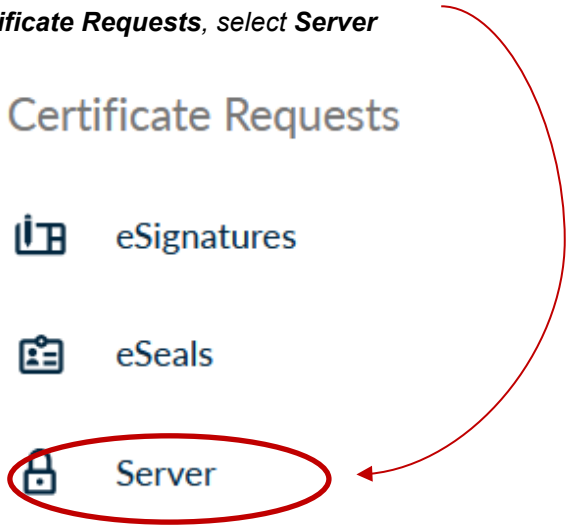


Melden Sie sich mit Ihrem **Hohenheimer Benutzerkonto** an

Log in with your Hohenheim user account

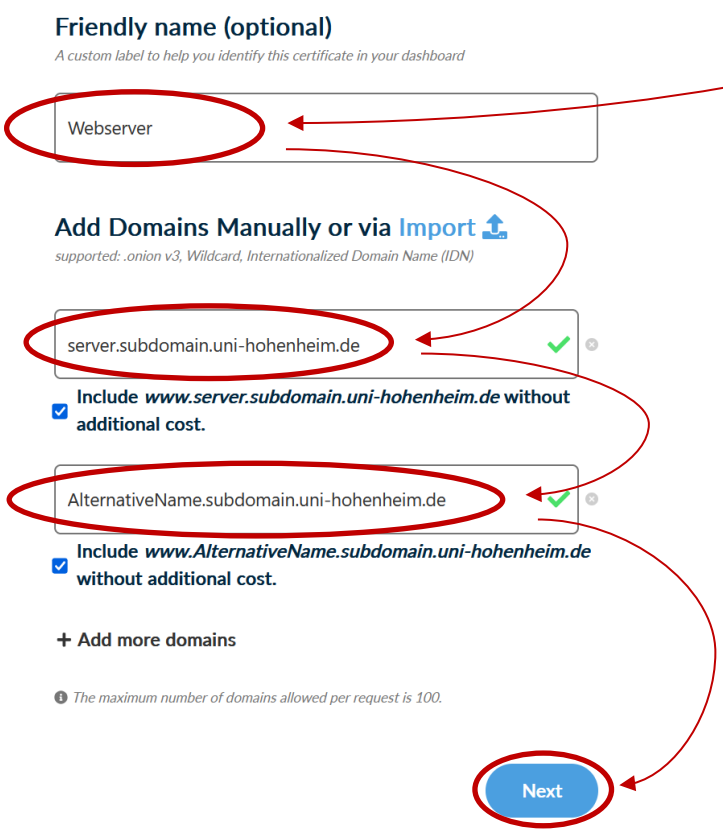
Wählen Sie auf der linken Seite unter **Certificate Requests Server**

*On the left-hand side, under **Certificate Requests**, select **Server***



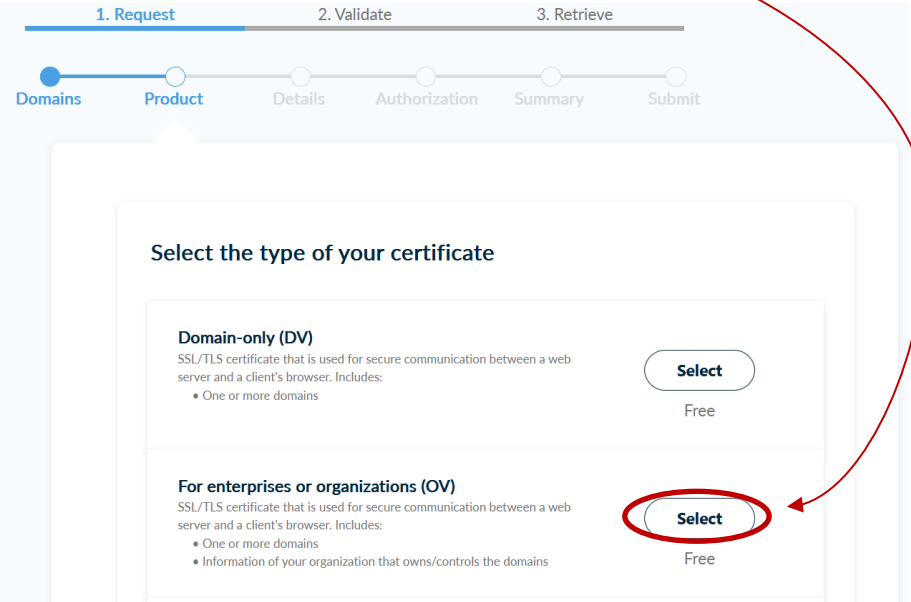
Geben Sie einen **Friendly name** (Zur späteren leichteren Identifikation, vor allem wenn Sie später mehrere Zertifikate besitzen) und den oder die **FQDN(s)** an.
Derzeit sind **maximal 100 FQDNs erlaubt!**

*Enter a **Friendly name** (for easier identification later, especially if you have several certificates later) and the **FQDN(s)***
*A **maximum of 100 FQDNs are currently permitted**!*



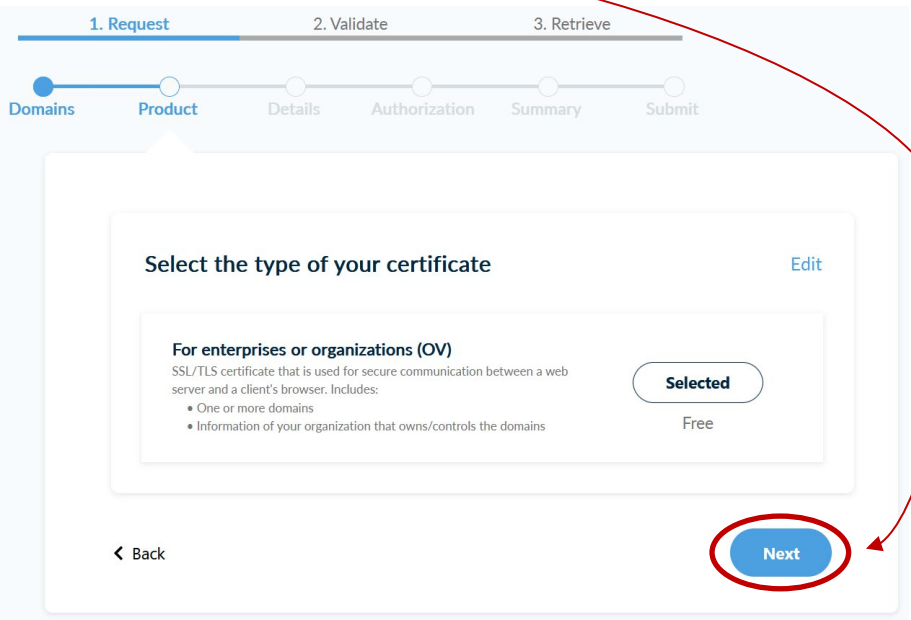
Wählen Sie **For enterprises or organizations (OV)**

*Select **For enterprises or organisations (OV)***



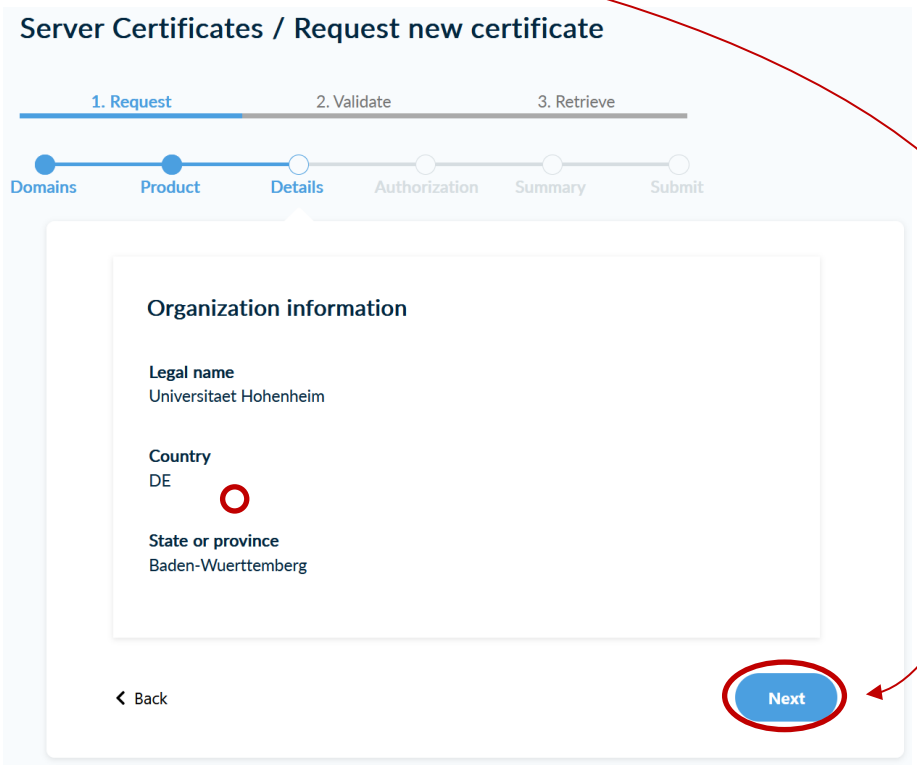
Wählen Sie **Next**

*Select **Next***



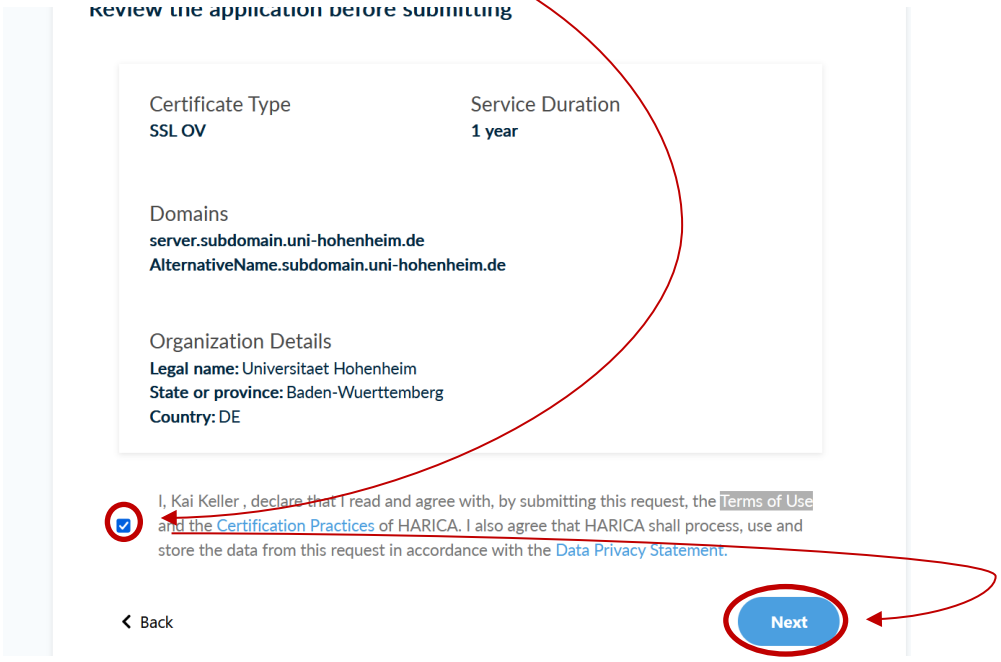
Wählen Sie nochmals **Next**

*Select **Next** again*



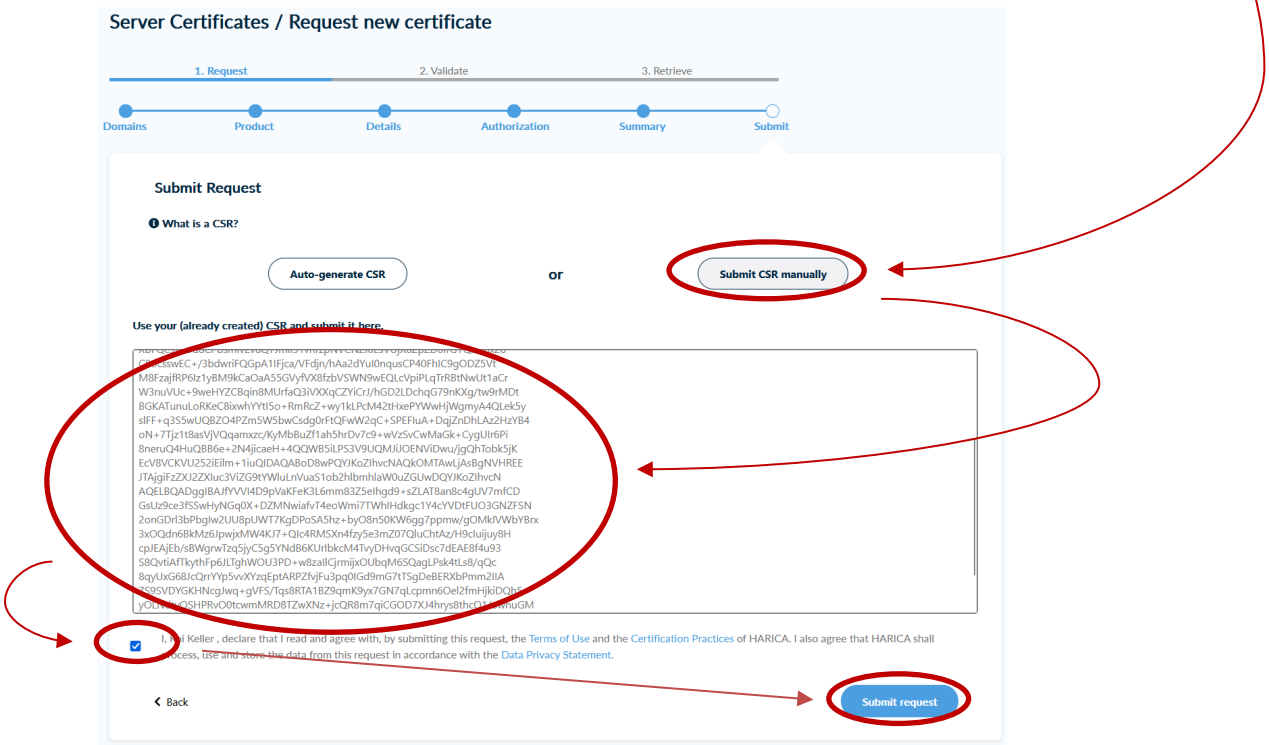
Akzeptieren Sie **Nutzungsbedingungen** und wählen Sie **Next**

Accept terms of use** and select **Next



Fügen Sie nun den **Inhalt** der **.csr-Datei** nach einem Klick auf **Submit CSR manually** in das Textfeld ein, **bestätigen** Sie nochmals die **Nutzungsbedingungen** und wählen Sie **Submit request.** Den Inhalt der .csr-Datei können Sie mit einem beliebigen Texteditor (bspw. Editor (Windows), Word, Notepad++) öffnen.

*Now insert the **content** of the **.csr file** into the text field after clicking on **Submit CSR manually**, **confirm the terms of use** again and select **Submit request.** You can open the content of the .csr file with any text editor (e.g. Editor (Windows), Word, Notepad++).*



Sobald wir das Zertifikat genehmigt haben, erhalten Sie eine **E-Mail vom Harica Certificate Manager (CM) bzw. von der E-Mail-Adresse noreply@harica.gr mit Betreff: HARICA – Your Certificate is ready und nebenstehendem, beispielhaften Inhalt.**

*As soon as we have approved the certificate, you will receive an **e-mail from the Harica Certificate Manager (CM) or from the e-mail address noreply@harica.gr with the subject: HARICA - Your Certificate is ready** and the following sample content.*

```
Your certificate is ready

Domains:

alternativename.subdomain.uni-hohenheim.de
server.subdomain.uni-hohenheim.de

In order to retrieve your certificate you have to download it from your
Dashboard <https://cm.harica.gr/MyDashboard>.

Do you need any assistance? Please contact us here!

Email support@harica.gr <mailto:support@harica.gr>
Telephone +30 2310 995000 <tel:+30 2310 995000>
```

Öffnen Sie nun die URL https://cm.harica.gr/MyDashboard oder klicken Sie auf den gleichnamigen Link. Evtl. müssen Sie sich erneut mit Ihrem Hohenheimer Benutzerkonto anmelden wenn Ihre Session bereits abgelaufen ist.

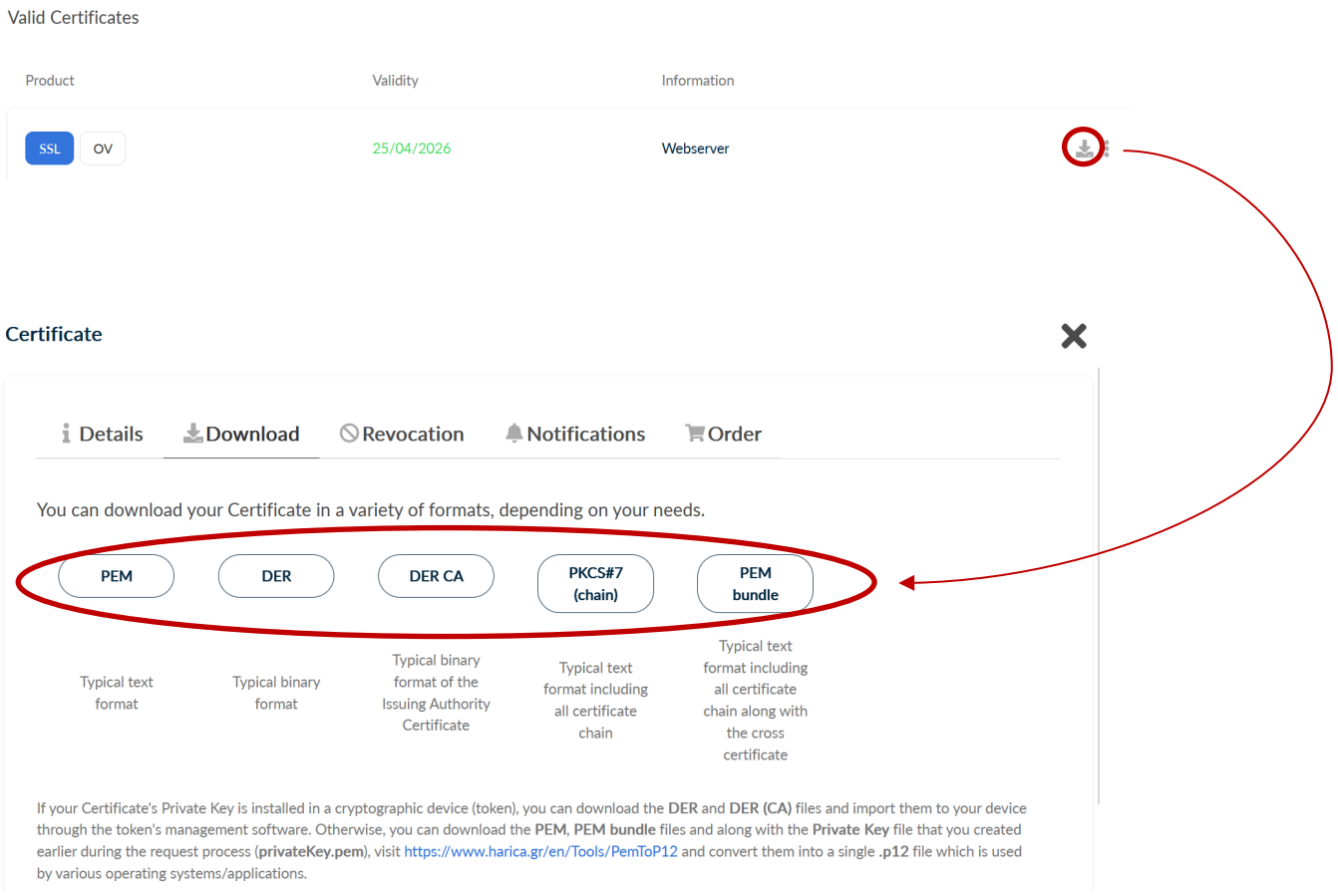
Unter **Valid Certificates** sollten Sie nun einen Eintrag für Ihr beantragtes Zertifikat finden und können ganz rechts mit dem **Download-Button** Ihr Zertifikat in **verschiedensten Formaten herunterladen.**

Außerdem finden Sie unter den einzelnen **Karteireitern weitere, interessante Informationen** zu Ihrem Zertifikat wie bspw. Gültigkeitsdauer, Benachrichtigungsinformationen und auch eine Möglichkeit das Zertifikat selbst zu sperren.

Now open the URL https://cm.harica.gr/MyDashboard or click on the link of the same name.
You may have to log in again with your Hohenheim user account if your session has already expired.

*Under **Valid Certificates** you should now find an entry for your requested certificate and can download your certificate in **various formats** using the **download button** on the far right.*

*You will also find **further interesting information about your certificate under the individual tabs**, such as validity period, notification information and also the option to revoke the certificate itself.*



Sollten unerwartete Probleme auftreten stehen wir Ihnen gerne am
KIM IT-Service-Desk
Biogebäude 1, Garbenstraße 30, 1. UG
per E-Mail unter
kim-it@uni-hohenheim.de
zur Verfügung

Should unexpected problems arise, we will be happy to help you at the
KIM IT-Service-Desk
Biogebäude 1, Garbenstraße 30, 1. Basement
email us at
kim-it@uni-hohenheim.de