



Serverzertifikate

Server certificates

Bezug von SSL- Serverzertifikaten

Obtaining SSL server certificates

19.05.2025

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

Inhalt

Voraussetzungen / <i>Prerequisites</i>	1
CSR erstellen / Create CSR	1
Bezug des SSL-Serverzertifikats / Obtaining the SSL server certificate	3

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](#))*

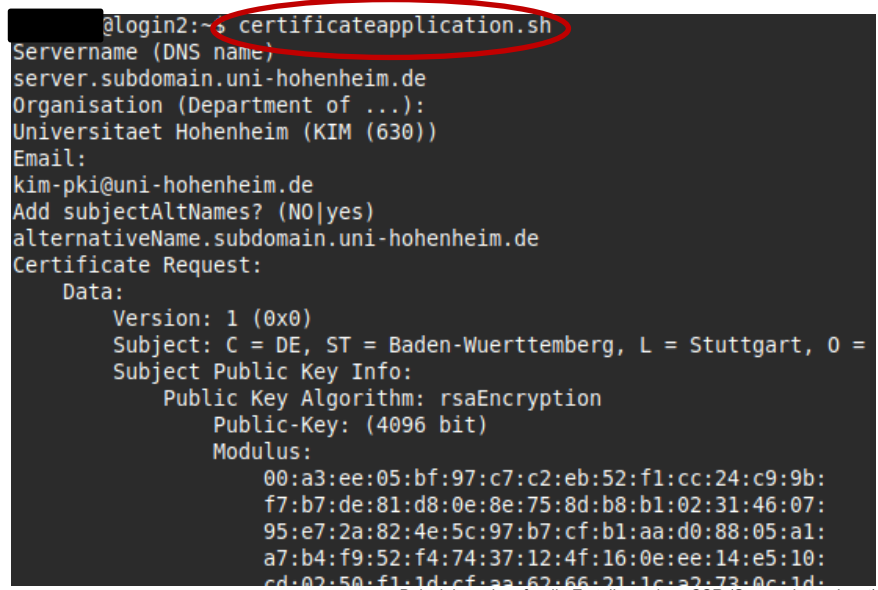
CSR erstellen / Create CSR

CSR Certificate Signing Request

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`:



```
@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:62:66:21:16: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**

Login

New to HARICA? [Sign Up](#)

Email address

Password

[Forgot password?](#)

Login

Or

Academic Login

Sign in

Wählen Sie **Universität Hohenheim**

Choose *University of Hohenheim*

Wählen Sie Ihre Institution aus

Vorherige Institutionen

	Universität Hohenheim uni-hohenheim.de
--	---

[+ Eine weitere Institution hinzufügen](#) [Bearbeiten](#)



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

Log in with your Hohenheim user account

The screenshot shows the HARICA login interface. The 'Benutzername' (Username) field is circled in red, with a red arrow pointing to it from the instruction text. The 'Passwort' (Password) field is also circled in red, with a red arrow pointing to it. Below the password field, there are two checkboxes: 'Anmeldung nicht speichern' (Do not save login) and 'Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.' (Show the information to be transmitted so that I can refuse its further processing if necessary). The 'Anmelden' (Login) button is circled in red, with a red arrow pointing to it. The HARICA logo and the text 'Hellenic Academic and Research Institutions Certification Authority' are at the top.

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

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

Certificate Requests

 eSignatures

 eSeals

 **Server**

Kommunikations-, Informations- und Medienzentrum (KIM)

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!

Friendly name (optional)
A custom label to help you identify this certificate in your dashboard

Webserver

Add Domains Manually or via Import 
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

server.subdomain.uni-hohenheim.de ✓

☒ Include **www.server.subdomain.uni-hohenheim.de** without additional cost.

AlternativeName.subdomain.uni-hohenheim.de ✓

☒ Include **www.AlternativeName.subdomain.uni-hohenheim.de** without additional cost.

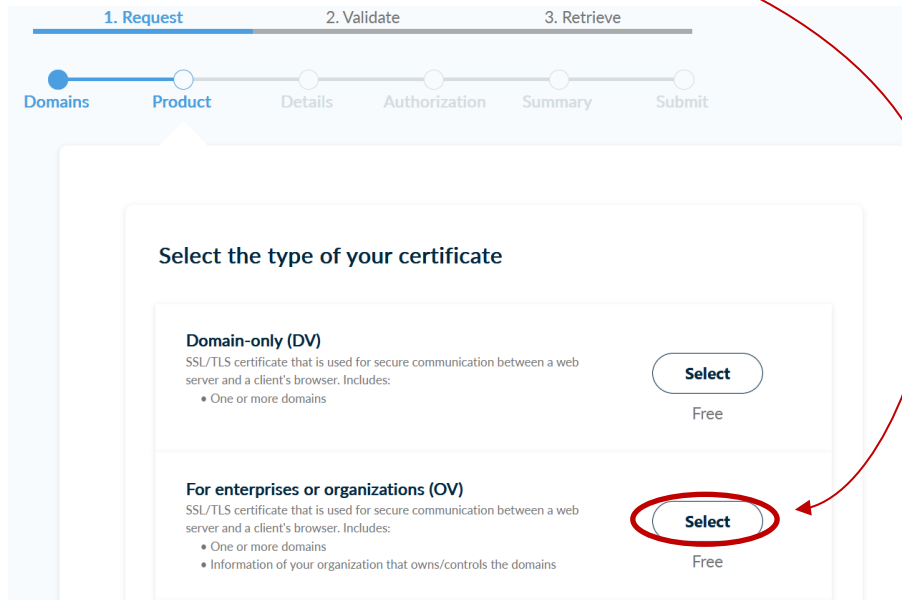
+ Add more domains

ⓘ The maximum number of domains allowed per request is 100.

Next

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

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



1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Select the type of your certificate

Domain-only (DV)
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
• One or more domains

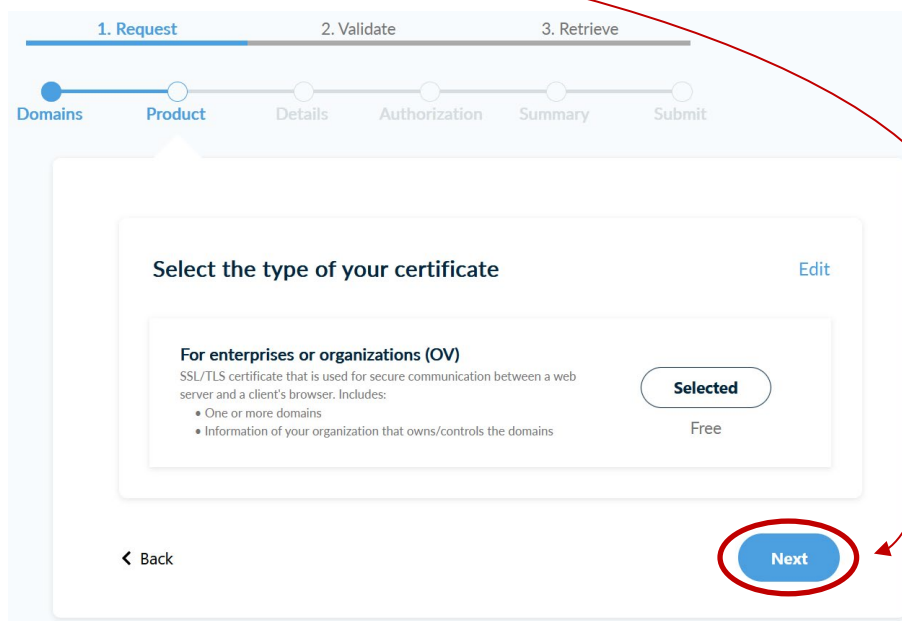
Select
Free

For enterprises or organizations (OV)
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
• One or more domains
• Information of your organization that owns/controls the domains

Select
Free

Wählen Sie **Next**

*Select **Next***



1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Select the type of your certificate

Edit

For enterprises or organizations (OV)
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
• One or more domains
• Information of your organization that owns/controls the domains

Selected
Free

< Back

Next

Kommunikations-, Informations- und Medienzentrum (KIM)

Wählen Sie nochmals **Next**

Select **Next** again

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Organization information

Legal name
Universitaet Hohenheim

Country
DE

State or province
Baden-Wuerttemberg

< Back **Next**

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

Accept **terms of use** and select **Next**

review the application before submitting

Certificate Type SSL OV	Service Duration 1 year
-----------------------------------	-----------------------------------

Domains
server.subdomain.uni-hohenheim.de
AlternativeName.subdomain.uni-hohenheim.de

Organization Details
Legal name: Universitaet Hohenheim
State or province: Baden-Wuerttemberg
Country: DE

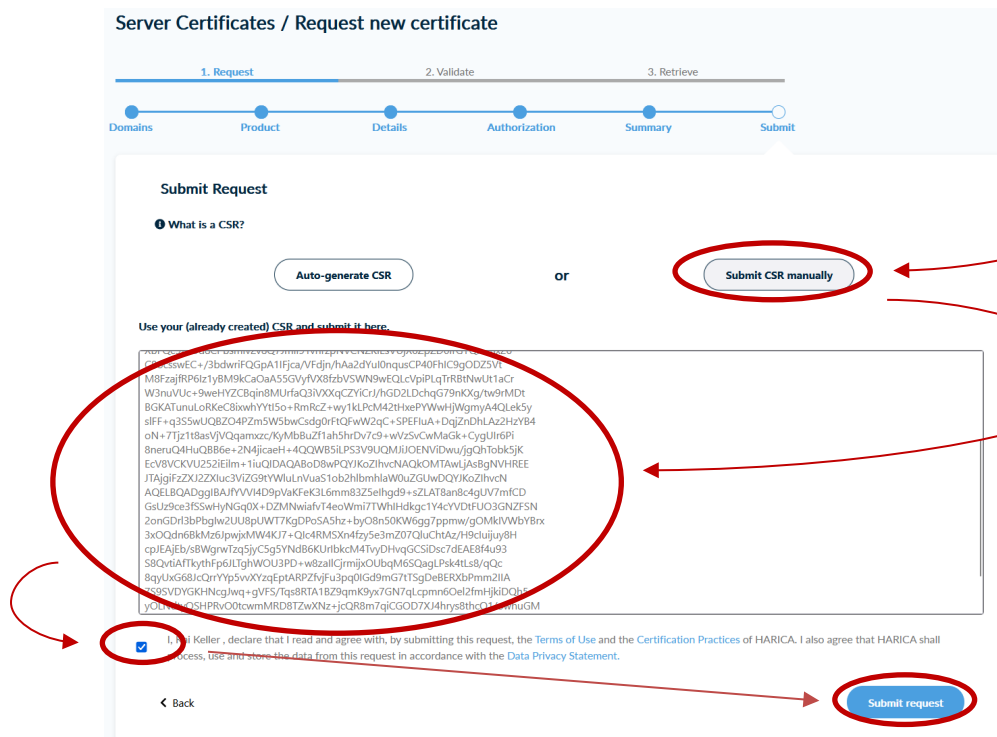
☒ I, Kai Keller, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

< Back **Next**

Kommunikations-, Informations- und Medienzentrum (KIM)

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:

alternativenname.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](tel:+30_2310_995000)>

Kommunikations-, Informations- und Medienzentrum (KIM)

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.*

Valid Certificates

Product	Validity	Information
SSL OV	25/04/2026	Webserver

Certificate

[Details](#) [Download](#) [Revocation](#) [Notifications](#) [Order](#)

You can download your Certificate in a variety of formats, depending on your needs.

PEM

DER

DER CA

PKCS#7 (chain)

PEM bundle

Typical text format

Typical binary format

Typical binary format of the Issuing Authority Certificate

Typical text format including all certificate chain

Typical text format including all certificate chain along with the cross certificate

If your Certificate's Private Key is installed in a cryptographic device (token), you can download the DER and DER (CA) files and import them to your device through the token's management software. Otherwise, you can download the PEM, PEM bundle files and along with the Private Key file that you created earlier during the request process (privateKey.pem), visit <https://www.harica.gr/en/Tools/PemToP12> and convert them into a single .p12 file which is used by various operating systems/applications.



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